UNIVERSIDADE FEDERAL DO AMAZONAS
FACULDADE DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

TALITA CAVALCANTE PINHEIRO

ACESSO E COMPARTILHAMENTO DE DADOS DE SAÚDE EM BLOCKCHAIN USANDO SMART CONTRACTS

MANAUS
2024

UNIVERSIDADE FEDERAL DO AMAZONAS
FACULDADE DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

TALITA CAVALCANTE PINHEIRO

ACESSO E COMPARTILHAMENTO DE DADOS DE SAÚDE EM BLOCKCHAIN USANDO SMART CONTRACTS

Dissertação apresentada ao Curso de Mestrado em Engenharia Elétrica, área de concentração em Controle e Automação de Sistemas na linha de pesquisa em Sistemas Inteligentes e Microeletrônica do Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas.

Orientador: Prof. Dr. Carlos Augusto de Moraes Cruz

MANAUS
2024

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Pinheiro, Talita Cavalcante
P654a Acesso e compartilhamento de dados de saúde em blockchain usando smart contracts / Talita Cavalcante Pinheiro . 2024
65 f.: il. color; 31 cm.

Orientador: Carlos Augusto de Moraes Cruz
Dissertação (Mestrado em Engenharia Elétrica) - UniversidadeFederal do Amazonas.

1. Blockchain. 2. Gestão de Saúde. 3. Contratos Inteligentes. 4.Registros Eletrônicos de Saúde(EHR). 5. Internet das Coisas Médicas (IoMT). I. Cruz, Carlos Augusto de Moraes. II. Universidade Federal do Amazonas III. Título

Poder Executivo
Ministério da Educação
Universidade Federal do Amazonas
Faculdade de Tecnologia
Programa de Pós-graduação em Engenharia Elétrica

TALITA CAVALCANTE PINHEIRO.

ACESSO E COMPARTILHAMENTO DE DADOS DE SAÚDE EM BLOCKCHAIN USANDO SMART CONTRACTS

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Engenharia Elétrica na área de concentração Controle e Automação de Sistemas.

Aprovada em 25 de março de 2024.

BANCA EXAMINADORA

Prof. Dr. Carlos Augusto de Moraes Cruz
Presidente
Universidade Federal do Amazonas

Prof. Dr. Roberta Lins Gonçalves, Membro
Universidade Federal do Amazonas

Prof. Dr. Frederico da Silva Pinagé, Membro
Universidade Federal do Amazonas

PPGEE
Programa de Pós-Graduação em Engenharia Elétrica - UFAM

Pós-Graduação em Engenharia Elétrica.
Av. General Rodrigo Octávio Jordão Ramos, nº 3.000 - Campus Universitário, Setor Norte - Coroado, Pavilhão do CETELI.
Fone/Fax (92) 99271-8954 Ramal:2607. E-mail: ppgee@ufam.edu.br

AGRADECIMENTOS

A Deus, minha fonte de graça. O primeiro a depositar confiança na realização deste trabalho. E a Nossa Senhora pela valorosa intercessão com que enriqueceu minha colaboração neste trabalho, ornando de méritos para que fosse entregue a seu Filho Jesus com toda dignidade.

À minha mãe, Maria de Fátima, meu apoio incondicional e exemplo de força e dedicação. Sua presença constante em minha vida foi alicerce que me permitiu alcançar este momento. Em honra à sua memória, sigo perseverante nos próximos passos.

Ao meu orientador, Professor Dr. Carlos Cruz, agradeço por sua orientação sábia, paciência e genialidade intelectual, que foram fundamentais neste percurso acadêmico. Sua orientação e entusiasmo moldou meu crescimento e me inspira a cada dia a superar novos desafios. À Prof. Dra. Roberta Gonçalves pela valiosa contribuição, o qual enriqueceu minha compreensão e perspectivas sobre as relevantes contribuições deste trabalho à sociedade.

Ao meu esposo Charles, meu filho Thiago e meu pai Vanildo, dedico este momento de conquista. Sobretudo ao meu esposo, apoio incondicional, me impulsionando nos momentos mais desafiadores.

À minha formadora pessoal e irmã de comunidade Hallel, Edlamar Benevides, que com sua orientação espiritual e motivação foram fundamentais para meu fortalecimento.

Aos queridos colegas de trabalho da Ufam, Ronaldo Ferreira, por sua obstinada insistência e apoio e à Jéssica Mariella, pela colaboração e companheirismo nos momentos mais desafiadores.

Agradeço à Universidade Federal do Amazonas (UFAM) e ao Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) pelo apoio concedido à minha pesquisa. A colaboração dos profissionais e dos recursos fornecidos por essa instituição que foram fundamentais para o desenvolvimento e sucesso deste trabalho acadêmico.

RESUMO

O avanço da tecnologia digital tem desempenhado um papel essencial no campo da saúde. A troca segura e eficiente de informações médicas é de relevante importância para garantir tratamentos eficazes na gestão de saúde. Considerando os avanços recentes no setor da saúde com a Internet das Coisas Médicas, a introdução de dispositivos vestíveis (wearables) e, mais recentemente, os ingeríveis, e os tradicionais Registros Eletrônicos de Saúde (EHR), faz-se necessário um gerenciamento para esses dados, a fim de que somente pessoas autorizadas tenham acesso. Há o desafio da interoperabilidade dos dados médicos entre várias instituições de saúde, e garantir a transmissão segura desses dados tornou-se uma prioridade devido aos ataques cibernéticos realizados por hackers. Essas informações são altamente confidenciais e valiosas no mercado, suscetíveis a extorsões. A Blockchain surge como uma potencial revolução na indústria da saúde, oferecendo recursos como privacidade e transparência de dados. Para controlar as informações geradas por diversos dispositivos médicos e os variados dados de saúde com diferentes origens, como exames de imagem, testes laboratoriais etc., propomos a utilização de Contratos Inteligentes baseados em Blockchain para acesso e compartilhamento seguro de dados, podendo permitir que os pacientes controlem quem pode acessar seus dados médicos e em quais circunstâncias. O sistema utilizará a plataforma de desenvolvimento sCrypt, uma estrutura para o desenvolvimento de aplicações em blockchain baseado no protocolo Bitcoin com a criação de Contratos Inteligentes (Smart Contracts). Uma aplicação que registrará e armazenará todos os eventos na blockchain, com um histórico imutável e com acesso global das informações médicas de qualquer lugar a qualquer momento.

Palavras-chaves: Blockchain; Gestão de Saúde; Contratos Inteligentes; Registros Eletrônicos de Saúde (EHR); Internet das Coisas Médicas (IoMT).

ABSTRACT

The advancement of digital technology has played an essential role in the field of healthcare. The secure and efficient exchange of medical information is of significant importance to ensure effective treatments in healthcare management. Considering the recent advancements in the healthcare sector with the Internet of Medical Things, the introduction of wearable and, more recently, ingestible devices, along with the traditional Electronic Health Records (EHR), it is necessary to manage these data to ensure that only authorized individuals have access. There is a challenge of interoperability of medical data among various healthcare institutions, and ensuring the secure transmission of these data has become a priority due to cyberattacks carried out by hackers. This information is highly confidential and valuable in the market, susceptible to extortion. Blockchain emerges as a potential revolution in the healthcare industry, offering features such as data privacy and transparency. To control the information generated by various medical devices and the diverse healthcare data from different sources, such as imaging exams, laboratory tests, etc., we propose the use of Blockchain-based Smart Contracts for secure access and sharing of data, enabling patients to control who can access their medical data and under what circumstances. The system will utilize the sCrypt development platform, a framework for developing blockchain applications based on the Bitcoin protocol with the creation of Smart Contracts. An application that will record and store all events on the blockchain, with an immutable history and global access to medical information from anywhere at any time.

Palavras-chaves: Blockchain; Healthcare Management; Smart Contracts; Electronic Health Records (EHR); Internet of Medical (Things IoMT).

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

API	*Application Programming Interface*
BSV	*Bitcoin Satoshi Vision*
BTC	*Bitcoin*
BVM	*Bitcoin Virtual Machine*
BCH	*Bitcoin Cash*
BaaS	*Blockchain as a Service*
DSA	*Digital Signature Algorithm*
DER	*Distinguished Encoding Rules*
DNS	*Domain Name System*
DICOM	*Digital Imaging and Communications in Medicine*
EHR	*Electronic Health Records*
EMR	*Electronic Medical Record*
EdDSA	*Edwards-curve Digital Signature Algorithm*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EVM	*Ethereum Virtual Machine*
GPToken	*General Purpose Token*
HMAC	*Hash-based Message Authentication Code*
HIPAA	*Health Insurance Portability and Accountability Act*
HHS	*Department of Health and Human Services*
iDIN	*IDentification In The Netherlands*
IEEE	*Institute of Electrical and Electronics Engineers*
IBM	*International Business Machines Corporation*
IoT	*Internet of Things*
IoMT	*Internet das Coisas Médicas*
LSHC	*Life Science and Healthcare*
MiCA	*Markets in Crypto-Assets*
NFT	*Non-Fungible Token*

ONC	*Office of the National Coordinator*
POW	*Proof of Work*
P2P	*Peer-to-peer*
PI	*propriedade intelectual*
PCOR	*Patient Care and Outcomes Research*
PHI	*Protected Health Information*
PII	*Personally Identifiable Information*
RIPEMD	*Race Integrity Primitives Evaluation Message Digest*
RGPD	*Regulamento Geral de Proteção de Dados*
RSA	*Rivest-Shamir-Adleman*
SHA	*Secure Hash Algorithm*
SAT	*Satoshis*
SegWit	*Segregated Witness*
TXID	*Transaction Identication*
TPS	*Transações por segundo*
UE	*União Europeia*
UTXO	*Unspent Transaction Output*

SUMÁRIO

1 INTRODUÇÃO

O crescimento da informação digital tem sido fundamental no avanço contemporâneo, especialmente na área da saúde. A transferência segura e eficiente de dados médicos é crucial para diagnósticos precisos e tratamentos eficazes. A digitalização e compartilhamento de dados têm remodelado a abordagem dos profissionais de saúde, melhorando a coleta, armazenamento e análise de informações clínicas, resultando em serviços mais eficientes e personalizados [1].

A produção de dados de saúde, provenientes de diversas fontes como registros clínicos, exames de imagem, testes laboratoriais e dispositivos Wearables, geram desafios significativos de padronizações e interoperabilidade entre instituições de saúde, devido a heterogeneidade nos formatos. A limitada capacidade de comunicação entre instituições e a interoperabilidade de Registros Eletrônicos de Saúde (EHR), representam obstáculos a integração dos dados de saúde, dificultando a troca eficiente de informações médicas entre diferentes sistemas e impedindo uma visão completa e integrada da saúde do paciente [1, 2].

Além disso, há a preocupação com a segurança na transmissão desses dados, devido às ameaças de ciberataques. Dados altamente sensíveis tornam-se alvos atrativos para hackers em busca de extorsão e fraudes médicas. Indivíduos mal-intencionados podem explorar dados para descobrir a localização dos pacientes, identificar condições de saúde, compreender rotinas de tratamentos. Apesar das oportunidades oferecidas pela produção massiva de dados de saúde, é crucial enfrentar esses desafios para garantir o pleno aproveitamento das possibilidades promissoras da era digital na área da saúde [1,2].

Considerando que o setor de saúde lida com informações confidenciais e busca tecnologias seguras, propõe-se a implementação de uma solução que ofereça controle efetivo sobre os dados. Uma solução que permita que os pacientes monitorem e controlem suas próprias informações, ao mesmo tempo em que equilibre interoperabilidade com privacidade e segurança. Essa abordagem é viabilizada pela tecnologia Blockchain.

Essa tecnologia, originalmente concebida para garantir transações financeiras seguras pela internet e sem necessidade de intermediários, teve sua primeira aplicação no mercado do Bitcoin. Inicialmente focada no setor financeiro, sua aplicabilidade rapidamente se expandiu para além das transações monetárias, à medida que sua capacidade de oferecer segurança e descentralização despertou interesse em diversos setores [3].

A Blockchain, além de aplicações médicas, também tem sido cada vez mais adotada em ambientes de Internet das Coisas (IoT) e em fábricas industriais, onde sua capacidade de

garantir segurança, transparência e integridade de dados se mostra crucial para operações eficientes e confiáveis [4,5,6].

A Blockchain utiliza Contratos Inteligentes (Smart Contracts), para garantir acesso exclusivo a pessoas autorizadas, estabelecendo controle preciso sobre as informações de saúde. Os usuários podem definir as condições sob as quais seus dados podem ser acessados, compartilhados ou utilizados por terceiros, garantindo poder de decisão sobre suas informações médicas. Esses contratos, estabeleçam regras para compartilhamento, escritos em linguagem de programação e armazenadas na blockchain, operam como leis, executando exatamente o que é acordado, e podem definir quem pode acessar os dados, em que condições, e por quanto tempo, e eliminando a necessidade de intermediários [4].

Os registros são imutáveis e transparentes, o que significa que todas as transações relacionadas aos dados de saúde são registradas de forma permanente e auditável. Isso representa uma excelente maneira de migrar os dados do paciente com segurança e integridade, além de manter essas informações acessíveis ao paciente ao longo de toda a sua vida. Isso porque, a partir do momento em que o bloco é inserido na cadeia, ele não pode ser modificado [7]. Portanto, caso seja necessário acrescentar uma nova informação, um novo bloco será criado, criando um histórico de informações, uma vez que permite auditar uma cadeia completa de informações que não são capazes de serem alteradas sem deixar nenhum tipo de rastro [8].

A tecnologia garante a interoperabilidade, unificando prontuários eletrônicos e diversas informações médicas. A descentralização garante o acesso aos seus dados independentemente de uma instituição, integrando os dados médicos e criando um histórico completo. Mesmo diante de problemas como falta de energia ou falhas de servidores, a natureza descentralizada da blockchain garante a operacionalidade do ecossistema, pois cada nó na rede mantém uma cópia completa do registro, com transações confirmadas e validadas por consenso entre os nós, os dados permanecem nos outros nós da rede [4, 6].

O setor da saúde enfrenta desafios relacionados à segurança, privacidade e interoperabilidade dos dados médicos. No entanto, com o avanço da tecnologia, especialmente com a emergência da Blockchain e dos Smart Contracts, novas oportunidades surgem para abordar esses desafios. Essa tecnologia promete revolucionar a interoperabilidade dos dados médicos, transformando a forma como os registros são armazenados, acessados e compartilhados. Ao promover a descentralização das transações em todos os setores da assistência médica, a Blockchain elimina restrições geográficas e proporciona um ambiente mais seguro para o gerenciamento de informações de saúde [6].

1.1 Objetivo Geral

Apresentar uma plataforma de teste fundamentada em Blockchain para garantir acesso e compartilhamento seguro de dados de saúde do paciente através de Smart Contracts, que estabelecem regras com controle de acesso ao paciente e autonomia para esse decidir quem pode acessar seus dados, seja profissionais de saúde ou outras partes envolvidas no processo.

1.2 Objetivos Específicos

- Implementar um ambiente de teste mediante Smart Contracts na plataforma Blockchain, visando que os pacientes controlem o acesso aos seus dados médicos, mediante concessão de permissões específicas para diferentes partes interessadas;
- Integrar a funcionalidade do protocolo da camada de aplicação Back-end do controle de acesso aos Smart Contracts com a interface de usuário;
- Estabelecer protocolos de segurança e criptografia para proteger os dados de saúde durante a transmissão e armazenamento na blockchain.

1.3 Organização do Trabalho

Este trabalho está organizado conforme a divisão descrita a seguir:

- Capítulo 1: Introdução;
- Capítulo 2: Revisão da Literatura;
- Capítulo 3: Referencial Teórico;
- Capítulo 4: Materiais e Métodos;
- Capítulo 5: Resultados e Discussões;
- Capítulo 6: Conclusão e Trabalhos Futuros;
- Capítulo 7: Referências Bibliográficas.

O capítulo 1 apresenta o contexto do trabalho, discorrendo sobre os problemas apresentados no setor da saúde, a relevância da Blockchain e as justificativas de que forma a tecnologia pode mitigar tais problemas. O capítulo 2, apresenta trabalhos relevantes na área de saúde com aplicações em Blockchain. O capítulo 3, apresenta os fundamentos teóricos das técnicas utilizadas no desenvolvimento deste trabalho. No capítulo 4, em materiais e métodos, detalhes da metodologia proposta, a plataforma de desenvolvimento e suas ferramentas. No capítulo 5 são apresentados os resultados alcançados e efetua-se uma discussão dos mesmos. No capítulo 6, a conclusão e sugestões de trabalhos futuros com recomendações de melhoria em relação ao método proposto e no capítulo 7, as referências utilizadas nesta dissertação.

2 REVISÃO DA LITERATURA

Para verificar quais as técnicas adotadas para o desenvolvimento da dissertação intitulada como “Acesso e Compartilhamento de Dados de Saúde em Blockchain usando Smart Contracts”, foi necessário realizar uma pesquisa bibliográfica a respeito do tema. Para essa busca os seguintes termos foram utilizados: "All Metadata":Access OR "All Metadata":Sharing OR "All Metadata":de Data) OR ("All Metadata":health data) OR ("All Metadata":BLOCKCHAIN) OR ("All Metadata":BSV) OR ("All Metadata":SMART CONTRACT, com anos da publicação de 2016 a 2023.

As pesquisas foram realizadas nas bases literárias IEEE (Institute of Electrical and Electronics Engineers) Xplore, Springer e Google Acadêmico. Os artigos foram obtidos utilizando a mesma estratégia de busca avançada com as devidas conversões e adaptações. Buscou-se principalmente por artigos de revista, por apresentarem maior credibilidade e confiabilidade, com anos da publicação de 2016 a 2023.

Nas seções iniciais deste capítulo, um breve contexto sobre a tecnologia blockchain, explorando os desafios enfrentados e as soluções promissoras que essa tecnologia oferece quando aplicada à área da saúde. Além disso, exemplos de sua aplicação em cenários médicos e artigos de revisão literária sobre uso da Tecnologia Blockchain manipulando dados médicos aplicados aos sistemas de saúde.

2.1 Contexto Histórico da Tecnologia Blockchain

O Bitcoin, surgiu em 31 de outubro de 2008, sendo o primeiro contato da comunidade científica com a blockchain através do white paper intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System". Nesse artigo, Satoshi Nakamoto, propôs uma nova criptomoeda, o bitcoin, para resolver o problema de gastos duplos através de uma abordagem peer-to-peer (P2P) e o Bitcoin tornou-se a primeira grande aplicação da blockchain [8].

A blockchain é um grande banco de dados compartilhado que registra as transações dos usuários. Em tradução livre, significa “corrente de blocos”, e o primeiro bloco da cadeia foi a geração com o bloco Gênese em 3 de janeiro de 2009 e a mineração do Bloco 1, mais tarde, em 9 de janeiro de 2009. Por volta de 2014, o foco da investigação científica passou do bitcoin para a própria Blockchain. Essa mudança resultou em diferentes versões da tecnologia com diferentes aplicações para além do mundo financeiro [8, 9].

Originalmente concebida para a criptomoeda “Bitcoin” e distinta dos bancos tradicionais por sua abordagem de armazenamento de dados, a tecnologia em sua essência, é

um sistema distribuído para registrar e armazenar transações, com registro compartilhado e imutável de transações peer-to-peer, construído a partir de blocos de transações vinculadas e armazenadas em um livro-razão digital. A tecnologia elimina a necessidade de uma autoridade central confiável, pois as transações são compartilhadas por todos os participantes da rede, usando um mecanismo de consenso e criptografia, com registros de data e hora. Esse processo elimina manipulação e disseminação de informações falsas na rede, criando um mecanismo contínuo de controle [10, 11].

As blockchains podem ser públicas, como no caso do Bitcoin e Ethereum, ou privadas. As blockchains públicas são acessíveis a todos, com informações de transações visíveis, normalmente usando Prova de Trabalho para garantir segurança, embora energeticamente mais intensivo e com exposição de informações publicamente. Já as blockchains privadas, restringem a participação e podem usar métodos de consenso diferentes, como Prova de Autoridade, aumentando a privacidade dos dados, mas limitando benefícios como a transparência total das informações como acontece na blockchain pública [10, 11].

Desde o surgimento da blockchain, várias ideias e aplicações foram propostas, despertando entusiasmo e preocupações. A tecnologia continua a evoluir com novos conceitos e casos de uso bem-sucedidos, apresentando-se como uma tecnologia disruptiva com o potencial de transformar mercados inteiros.

2. 1. 1 Relevância da tecnologia Blockchain na saúde

A indústria da saúde enfrenta desafios significativos, incluindo problemas de rede confiável, privacidade de dados, roubos de propriedade intelectual e interoperabilidade. A seguir, destaca-se alguns dos problemas que o setor enfrenta [11]:

Falta de rede confiável de dados: Não existe e, é necessária uma rede ponto a ponto para aumentar a eficiência na troca de documentação de dados.

Roubo de propriedade intelectual: É fundamental devido ao aumento da investigação colaborativa e da digitalização.

Privacidade de dados: As violações de dados expõem os registros de pacientes, uma vez que esses dados não encriptados e centralizados levam a problemas de privacidade.

Interoperabilidade: Existe falta de interoperabilidade entre as partes interessadas no ecossistema da saúde (médicos, farmácias etc.) devido a diferentes padrões de dados.

Atividades centradas no paciente: As partes interessadas têm apenas acesso limitado aos dados de saúde ou nenhum acesso. Dificuldades em acessar esses registros, principalmente quando estão fragmentados com diferentes prestadores de saúde.

Dadas as características singulares da blockchain, a indústria da saúde pode colher diversos benefícios. A tecnologia tem o potencial de solucionar ou reduzir consideravelmente esses problemas, a seguir algumas soluções [12]:

Registros médicos: O histórico médico de um paciente, fragmentado, poderia ser centralizado em uma blockchain.

Compartilhamento de receitas: Um paciente poderia consentir que suas prescrições pessoais fossem rastreadas para melhorar a transparência.

Testes clínicos: O rastreamento e os resultados poderiam ser direcionados para uma blockchain para melhorar a eficiência do desenvolvimento de tratamentos.

Cuidado baseado em valor: Rastrear o atendimento de um paciente e eventos médicos podem ser usados para determinar a qualidade do atendimento ao longo do tempo.

Atividades centradas no paciente: Contratos inteligentes para consentimento do paciente, gerenciamento de dados e de medicamentos prescritos; Segurança de dados para tecnologia vestível que transmitam informações do paciente em tempo real para monitorar e rastrear os resultados dos pacientes.

Anonimato do usuário: A criptografia permite manter ocultas as identidades.

Transparência aprimorada: Todos os participantes visualizam os dados adicionados. A integridade dos dados é melhorada por ser a única fonte da verdade.

Rastreabilidade: A transparência dos dados imutáveis permitem a permeação da informação ao longo da cadeia, diminuindo assim as falsificações.

Auditabilidade: dados de transações (por exemplo, dados de ensaios clínicos, rastreamento da cadeia de suprimentos) são armazenados de forma imutável e eterna.

Interoperabilidade: Através de contratos inteligentes, a comunicação entre as organizações de saúde podem ter o acesso aos dados armazenados de forma automatizada.

Credenciamento médico: As organizações credenciadoras poderiam acumular dados no livro-razão da blockchain e disponibilizá-los para outras organizações.

Considerando a abordagem apresentada, observou-se que o crescimento do mercado de saúde identificado em 2018 foi impulsionado pela necessidade crescente de transparência, segurança de dados, digitalização nos sistemas de saúde, e a descentralização tecnológica para reduzir custos e aumentar eficiência. O crescimento motivado na eliminação de desperdício e

na detecção de fraudes, resultou em avaliações que previam um aumento de mais de US$ 270 bilhões anualmente. O crescimento considera melhorias para combater práticas como faturamento excessivo, cobrança por serviços não realizados e fornecimento de informações falsas [11, 13].

O mercado demonstra um crescimento significativo e até final de 2022, o investimento em blockchain em diversos setores ultrapassaram mais de US$ 1 bilhão. Com um crescimento exponencial, este mercado deverá atingir globalmente US$ 67,4 bilhões até 2026. A indústria da saúde médica projeta um crescimento promissor até 2032, atingindo uma marca de aproximadamente US$ 14,25 bilhões, conforme figura 1 [14].

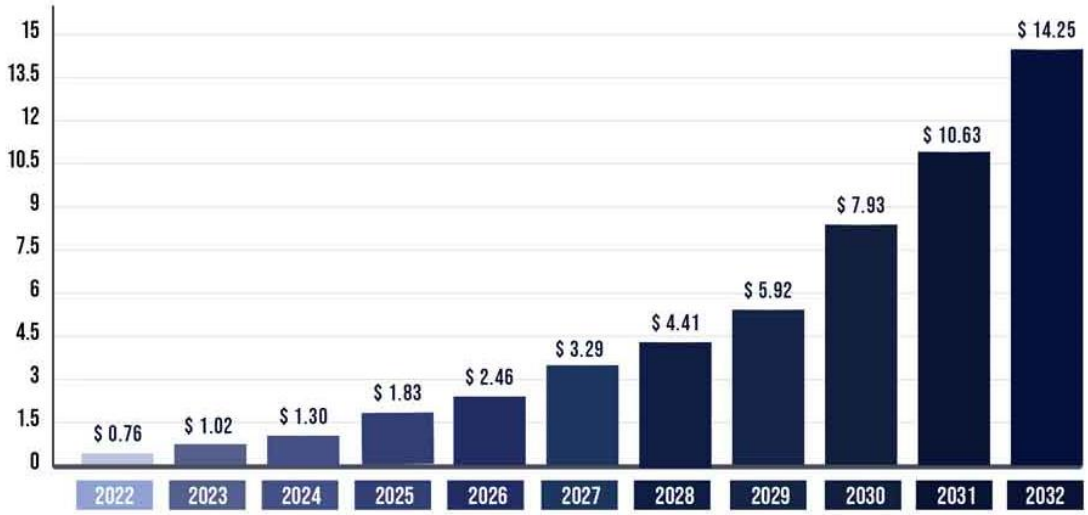

Figura 1: Projeção em bilhões da Blockchain no mercado de saúde de 2023 até 2032.

Fonte: Predence Research, 2023.

Os crescentes problemas com violações de dados de saúde durante a pandemia do covid, a ameaça de falsificações e a rápida demanda por transparência no ambiente de saúde estão alimentando o crescimento. À medida que mais empresas buscam melhorar a integridade de seus dados e a confiança do cliente, a tecnologia Blockchain se torna uma escolha atraente.

2.1.2 Abordando desafios e explorando possibilidades na blockchain

A viabilidade da blockchain nas empresas depende da capacidade de resolver desafios com partes de interesses conflitantes e compartilhamento de dados. Requer planejamento de aspectos operacionais e técnicos, como modelo de negócios, contratos inteligentes e escolha das redes, enquanto enfrenta diversos desafios.

Um dos primeiros desafios a ser vencido é a escalabilidade, pois muitos dos processos exigiriam mais escalabilidade e equilíbrio entre redes blockchains sem permissão e blockchains com permissão. Em 2016, a blockchain do Bitcoin processava cerca de sete transações por segundo, apesar de contar com mais de 10 milhões de usuários e registrar 200 mil transações diárias. Em contraste, as blockchains autorizadas podem acelerar o processamento de transações, embora enfrentem limitações de poder computacional devido à participação restrita na rede [15, 16].

A escalabilidade é um desafio para as criptomoedas, especialmente as mais antigas. No final de 2017, o Bitcoin enfrentava altas taxas e lentidão nas transações, chegando a pagar cerca de US$ 28 em taxas para que suas transações não levassem dias para serem concluídas. Esses problemas resultaram em um hard fork e uma nova moeda baseada no Bitcoin surgiu, o Bitcoin Cash (BCH), que aumentou o tamanho máximo do bloco de 1 para 8 MB [16]. Contudo, em 2024 se encontra em mais 500 GB, conforme figura 2.

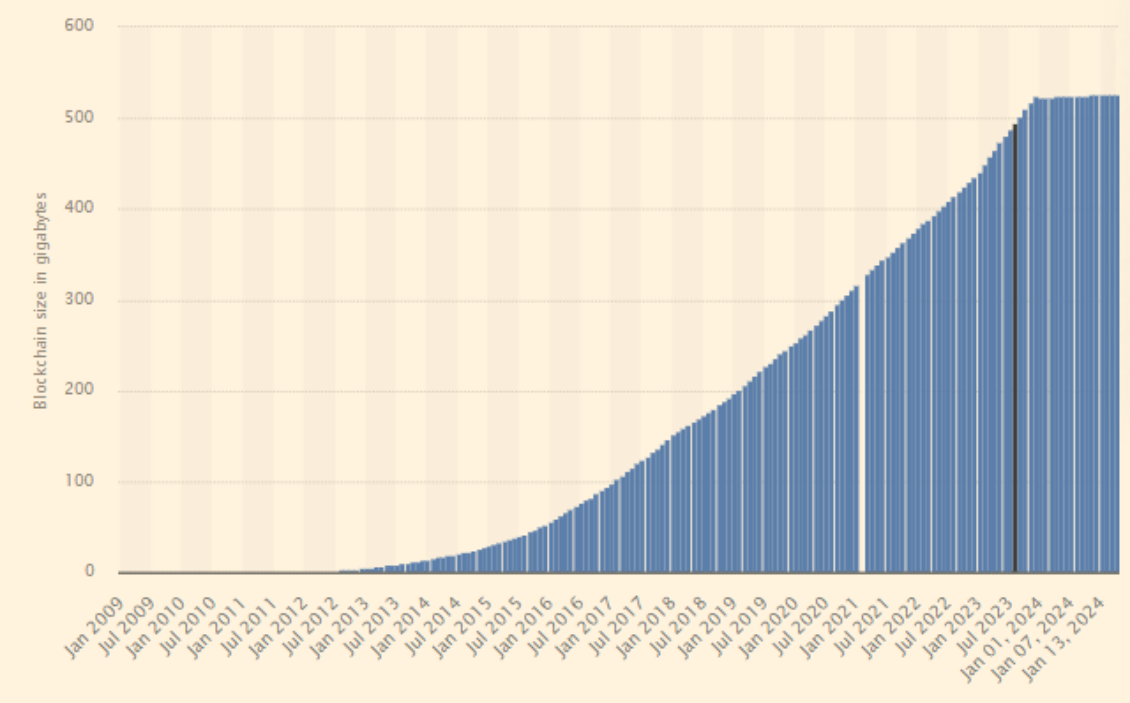

Figura 2: Tamanho da blockchain Bitcoin de jan de 2009 a 13 de jan de 2024.

Fonte: Statista, 2024.

Deve-se levar em consideração o escopo dos dados por meio de governança, o que implica controlar os tipos, tamanhos e formatos de dados que podem ser armazenados na blockchain. Pode ser eficaz operar com conjuntos de dados específicos, como informações demográficas e históricos médicos. Além disso, é importante considerar o consumo de poder

computacional para processar as transações, pois o custo está relacionado ao volume e tamanho das transações na rede. Incentivar provedores a adotar registros médicos eletrônicos pode facilitar a utilização eficiente da blockchain na área da saúde [10, 11, 15].

Com relação a escalabilidade, uma marca atingida pelo Bitcoin, foi no dia 8 de agosto de 2023, um recorde mundial, ao processar 128,691 milhões de transações em um período de 24 horas, demonstrando a viabilidade de escalar o protocolo Bitcoin original para lidar com uma quantidade significativa de transações na própria cadeia [16, 17]. Na figura 3, observa-se esse aumento significativo do número de transações de 2009 a 2023.

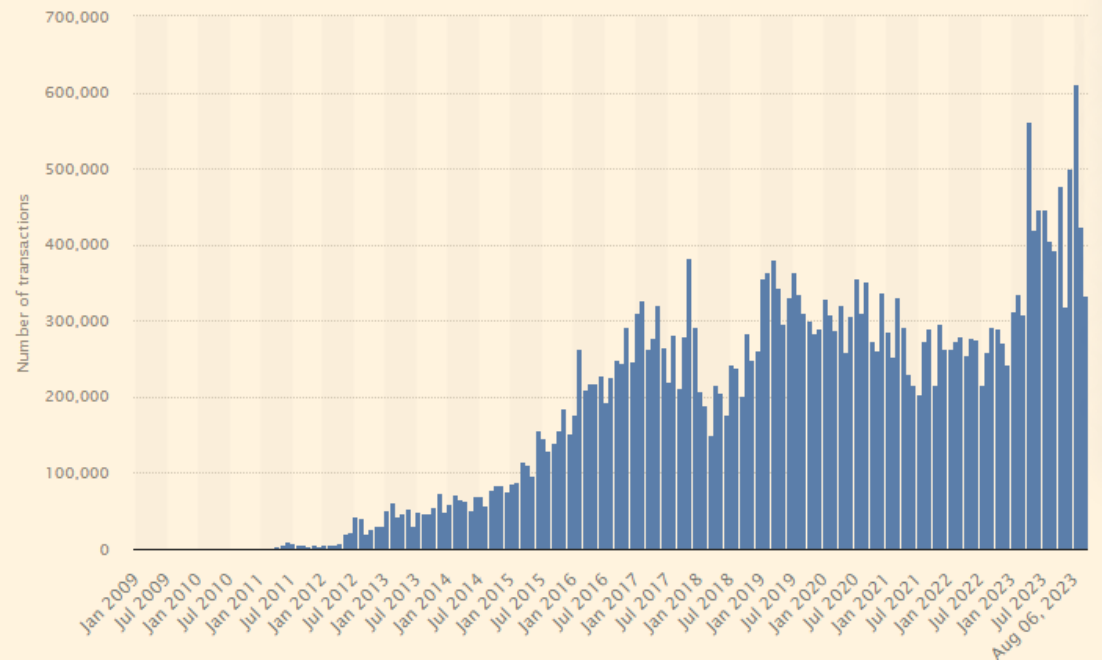

Figura 3: Transações diárias no Bitcoin de jan de 2009 a 8 de ago de 2023.

Fonte: Statista, 2023.

O aspecto financeiro é crucial, pois os investimentos em sistemas convencionais resultam em custos substanciais. No entanto, a blockchain com sua natureza de código aberto e distribuído, reduz os custos ao permitir o compartilhamento de recursos. Além disso, a imutabilidade dos registros elimina a necessidade de atualizações frequentes, já que todos os dados são registrados permanentemente, evitando custosas contingências de recuperação de dados presentes em sistemas tradicionais. Um desafio adicional está relacionado às considerações regulatórias, pois as estruturas atuais não colaboram para o crescimento do ecossistema blockchain. Isso inclui questões sobre a natureza do armazenamento distribuído da

tecnologia, a posse dos registros e as políticas de acesso. Em um sistema de informação compartilhado, a governança é crucial para determinar o proprietário dos dados [10].

Uma preocupação importante envolve a autorização de uso dos dados pelo paciente. O Departamento de Saúde e Serviços Humanos (HHS), por meio da Regra de Privacidade da HIPAA, a Lei de Portabilidade e Responsabilidade de Seguro de Saúde (Health Insurance Portability and Accountability Act) estabelece padrões para proteger a privacidade dos registros médicos dos indivíduos e impõe limites ao uso e divulgação desses registros. A solução aborda o desafio imposto pela Regra (HIPAA) ao separar e criptografar dados pessoais de saúde (PHI) e informações pessoalmente identificáveis (PII) [10,11].

Armazenar informações demográficas de alto nível na rede requer cuidado devido ao risco de identificação de pacientes, especialmente quando combinadas com dados de localização. Essas preocupações são mais significativas em áreas rurais, onde identificar indivíduos com condições de saúde raras pode ser mais fácil do que em áreas urbanas densamente povoadas. Uma solução parcial é a utilização de blockchains autorizadas [11].

A adoção generalizada da tecnologia requer tempo e comprometimento. Enquanto isso, as empresas podem iniciar a exploração dos benefícios por meio de iniciativas como, adquirir conhecimento em workshops colaborativos, priorizar recursos para casos de uso viáveis, envolver tomadores de decisão desde o início do design, e superar obstáculos regulatórios, como o Regulamento Geral de Proteção de Dados da União Europeia (RGPD).

A adoção da tecnologia enfrenta falta de conhecimento, incertezas legais e padronização. A criação de casos de negócios sólidos para justificar os altos custos de implementação é complicada devido ao ambiente regulatório rigoroso e à dependência de sistemas legados. Além disso, os requisitos das leis de proteção de dados entram em conflito com a imutabilidade, um desafio devido às características intrínsecas das blockchains [18].

O RGPD da UE (679/2016) concede aos indivíduos direitos de apagar e corrigir dados, em contraste com a imutabilidade da blockchain. Os dados armazenados em uma blockchain não podem ser facilmente excluídos ou alterados, o que levanta desafios para conformidade com o RGPD [19, 20].

Os resultados da pesquisa em resposta a um desafio de concepção proposto pelo Escritório do Coordenador Nacional de Tecnologia de Informação em Saúde (ONC) do Departamento de Saúde e Serviços Humanos indicam ações para promover a tecnologia na área de saúde, através de um ecossistema que reúna prestadores de cuidados de saúde, planos de saúde, empresas de ciências biológicas, startups e acadêmicos, com mecanismos para

identificar startups promissoras e facilitar a conexão com organizações experientes. Além disso, lições da indústria financeira podem auxiliar nos testes de blockchain para a troca de registros médicos eletrônicos, fornecendo informações valiosas aos decisores políticos antes da implementação em larga escala [11,15].

Essas ações incluem: Educação e gestão de habilidades; Rede e troca de conhecimento; Infraestruturas técnicas favorecendo a implementação; Incentivo financeiro ao uso da Blockchain e Regulamentação e padronização.

As incertezas legais e a falta de padronização são obstáculos. É fundamental estabelecer ambiente regulatório favorável com diretrizes específicas para o setor de saúde, em conformidade com regulamentos como o RGPD. Além disso, a harmonização com os padrões da UE para a blockchain, como o regulamento MiCA (Markets in Crypto-Assets) sobre Mercados de Criptoativos, é crucial para evitar fragmentação regulatória [10].

A seguir, será apresentada uma análise dos trabalhos com aplicações da Blockchain na Saúde Médica.

2.2 Soluções Médicas na Rede Blockchain

Apresentam-se resultados de aplicações pioneiras da blockchain na área da saúde, incluindo o MedRec e o PreScrypt em 2016, bem como o MedicalChain em 2018. Além disso, um white paper de 2016, intitulado como "Blockchain: Opportunities for Health Care" elaborado em resposta ao desafio de concepção proposto pelo ONC do Departamento de Saúde e Serviços Humanos (HHS) é analisado.

Em 2016, o white paper "Blockchain: Opportunities for Health Care", destacou-se como um dos artigos premiados dentre mais de 70 submissões provenientes de uma diversificada gama de indivíduos, organizações e empresas, todos explorando como a tecnologia pode ser aplicada na saúde. Esse white paper, estabeleceu diretrizes para o desenvolvimento de uma arquitetura baseada em blockchain para o setor médico [10].

Este white paper demonstra a troca de informações de saúde e o valor real da interoperabilidade. Apresenta casos promissores, tais como a Precision Medicine Initiative, Patient Care and Outcomes Research (PCOR) e o Nationwide Interoperability Roadmap. O artigo sugere um roteiro para dois casos de uso na blockchain: (1) verificar e autenticar informações e (2) transferir valor [10].

No primeiro uso, as organizações verificam a identidade digital, os dados genéticos ou o histórico de prescrições de um paciente. Na segunda aplicação, as organizações transferem um valor, como criptomoedas ou direitos de propriedade intelectual [10].

O PreScrypt, um exemplo de aplicação para prescrições médicas, destinado a pacientes com doenças crônicas, desenvolvida como prova de conceito pela Deloitte Holanda, em colaboração com o SNS Bank NV, Radboud3, e o REshape Center. Essa aplicação dá aos pacientes a propriedade total dos seus registros médicos, permitindo-lhes conceder e revogar o acesso dos seus dados e simplificar a aquisição e prescrição de medicamentos repetidos na Holanda, devido à ineficiência do sistema atual, que enfrentavam a repetição de renovações de prescrições [21, 22].

Os consumidores têm o controle para qual provedor de saúde compartilhar suas informações e para qual farmácia enviar suas receitas. O desafio era a ligação entre a identidade física do consumidor de saúde e sua identidade digital na blockchain. A SNS Bank NV resolveu esse problema conectando seu serviço IDIN (IDentification In The Netherlands) ao PreScrypt, um serviço de autenticação online. Isso permite que os usuários autentiquem sua identidade com a segurança do internet banking na blockchain [22].

Os fornecedores de medicamentos se beneficiam das transações registradas na blockchain, permitindo verificação instantânea da validade dos dados, incluindo a autenticidade das receitas médicas e o histórico de uso, com comunicação de dispositivos IoT (Internet of Things) via blockchain e a implementação de um Registro de Saúde [21,22].

O protótipo MedRec foi desenvolvido para gerenciar registros médicos eletrônicos com posse de dados e permissões de visualização. Utiliza contratos inteligentes para automatizar permissões de acesso ou criação de novos registros e lida com questões de compartilhamento de dados. Sua implementação aborda três problemas: o acesso fragmentado e lento aos dados, a falta de interoperabilidade e a falta de controle do paciente sobre seus dados. Os autores reuniram referências a dados médicos de diferentes fontes e as codificaram em uma blockchain Ethereum, com um histórico médico completo [23].

Utiliza contratos inteligentes para automatizar as alterações de status e protege cada registro por meio de um hash criptográfico. Centraliza as referências do paciente-provedor de um usuário, criando um único ponto de consulta de histórico médico. A identificação é confirmada por criptografia de chave pública, e uma implementação semelhante a DNS (Domain Name System) mapeia uma identificação existente (como número de seguro social)

para o endereço Ethereum da pessoa, usando strings em vez de chaves públicas criptográficas, garantindo compatibilidade com a identificação já em uso [23].

O MedRec pode receber dados de várias origens, sendo integrado em sistemas existentes ou em futuras infraestruturas. Ele disponibiliza APIs (Application Programming Interface) abertas para facilitar a revisão e a troca nos EHR. O uso de APIs melhora os repositórios de dados de saúde, possibilitando um "sistema de saúde de aprendizado" com aprendizado de máquina e análise de dados. Suporta análises para vigilância de doenças, alertas médicos para abuso de prescrições e coleta de dados de tratamentos. Simplifica a interoperabilidade ao adotar padrões abertos para a troca de dados e cumprir regulamentos como a HIPAA e se alinha com os objetivos do ONC de padrões de interoperabilidade [15].

Em 2017, a Change Healthcare lançou uma tecnologia blockchain em escala empresarial para o gerenciamento do ciclo de receitas em hospitais e sistemas de saúde.

Em 2018, os cuidados de saúde incluíram áreas, como combate a medicamentos falsificados, facilitação do licenciamento e compartilhamento de conhecimento técnico.

Abaixo, breves relatos de casos de uso para o ano de 2018, entre eles:

MedicalChain, utilizando uma arquitetura Hyperledger Fabric, baseada em níveis de permissões, permitindo mais controle e autonomia na visualização dos dados, através do qual o paciente permite quem irá visualizar os registros e por quanto tempo, para diferentes agentes de saúde, interagindo da maneira que julgar necessário.

Philips Healthcare fez parceria com a Gem para desenvolver aplicativos empresariais de saúde, como aplicativos de bem-estar e programas globais de identificação de pacientes; O serviço de manutenção de registros baseado em blockchain Factom fez parceria com o principal provedor de serviços médicos dos EUA, HealthNautica, para implantar uma solução para registros digitais; O Projeto MediLedger, envolvendo fabricantes de medicamentos, estabeleceu um sistema de rastreamento de medicamentos em uma blockchain compartilhada para prevenir a falsificação e o roubo de medicamentos; Exemplos notáveis incluem a Boehringer Ingelheim, que cooperou com a IBM (International Business Machines Corporation) para implementar uma solução de contabilidade blockchain para ensaios clínicos; A Bloqcube testou soluções que permitem que os participantes de ensaios clínicos recebam pagamentos, como moedas digitais emitidas por bancos centrais, para agilizar o processo de pagamento nos ensaios [15, 24, 25, 26, 27, 28].

A partir de 2022 observam-se os seguintes cenários, como segue:

A startup alemã PharmaTrace, inovou para proteger dados e implementar contratos inteligentes na indústria farmacêutica na plataforma Hyperledger Fabric. Seu principal produto é uma plataforma Blockchain as a Service (BaaS) que oferece soluções de fácil acesso, modelos personalizáveis de "plug and play" e escalabilidade para o setor farmacêutico; A empresa dos EUA, BurstIQ, oferece uma plataforma de informações de saúde pessoal em conformidade com o RGPD, usando blockchain e big data [11, 29].

Uma aplicação relevante que envolveu o gerenciamento seguro de registros médicos superando a fragmentação de dados entre sistemas de saúde e farmácias, é da empresa Guardtime, colaborando com autoridades de saúde da Estônia e do Reino Unido para rastrear e gerenciar consentimentos de pacientes. Eles transferiram 30 milhões de registros para a sua plataforma MyPCR, tornando-os acessíveis a pacientes e entidades autorizadas via smartphones. Essa plataforma melhorou a adesão à medicação no Reino Unido [30].

Na Alemanha, embora haja avanços na interoperabilidade, uma comparação internacional indica que ainda tem potencial de melhoria na interoperabilidade e digitalização em geral. Numa comparação global, os países como a Dinamarca, a Suécia ou a Finlândia têm uma grande vantagem graças às plataformas LSHC (Life Science and Healthcare) nacionais interoperáveis já estabelecidas. Os países como a Suíça ou a Áustria, também fizeram progressos significativos na implementação dos seus EHR [31].

Na tabela 1, observa-se artigos relevantes da aplicação da tecnologia blockchain na área médica de 2016 a 2022, sobretudo com a utilização de Contratos Inteligentes.

TÍTULO	ANO	PLATAFORMA	PROPÓSITO GERAL
MedRec: Using blockchain for Medical Data Access and Permission Management [32]	2016	Ethereum	Um sistema de prova de conceito baseado em contratos inteligentes aplicado aos EHR. Este sistema integra-se com os sistemas existentes dos provedores e visa desenvolver um protótipo destinado a oferecer aos pacientes registros médicos imutáveis de suas informações.
Secure and Trustable Electronic Medical Records Sharing using Blockchain [33]	2017	Rede privada da Ethereum	Gerenciamento de dados de saúde baseados em blockchain particular, para o compartilhamento de dados EHR entre prestadores de cuidados de saúde e para estudos de pesquisa.

Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring [34]	2018	Blockchain de consórcio na Ethereum	Integração de sensores, dispositivos inteligentes e contratos inteligentes para monitorar pacientes e registrar eventos em uma blockchain.
Secure storage and sharing of health data [35]	2018	Blockchain privada-XBlock	Modelo para armazenar e compartilhar informações de saúde em uma blockchain onde os usuários têm o papel de terminais.
A Secure Healthcare System Design Framework using Blockchain Technology [38]	2019	Blockchain privada	Implementação de um sistema de monitoramento e detecção, usando a Internet das Coisas (IoT) e a tecnologia blockchain como sistema de gerenciamento de transações e acesso.
Concessão de Permissão a Dados de Saúde Baseada em Blockchain [37]	2019	Hyperledger e Enigma	Blockchain e contratos inteligentes para garantir privacidade dos dados de saúde coletados no ambiente domiciliar de um paciente.
A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract [38]	2020	TESTRPC da Ethereum	Integração de IoT com sistemas de saúde remotos utilizando contratos inteligentes para gerenciar informações de pacientes e dispositivos médicos.
Blockchain Application in Healthcare [39]	2020	Blockchain Ethereum	Armazenamento de Registros Médicos Eletrônicos usando contratos inteligentes.
Towards a Remote Monitoring of Patient Vital Signs Based on IoT [40]	2020	Hyperledger	Monitoramento de sinais vitais de pacientes usando contratos inteligentes.
A Patient-Centric Health Information Exchange Framework Using Blockchain Technology [41]	2020	Blockchain Ethereum	Modelo de blockchain usando contrato inteligente para proteção de dados e fornecer aos pacientes controle total de seus registros.
A Blockchain based Electronic Medical Health Records Framework using Smart Contracts [42]	2021	Hyperledger Fabric	Infraestrutura baseada em Contratos Inteligentes para privacidade, acessibilidade e interoperabilidade de dados no setor de saúde por meio de EHR.

Applied Blockchain Technology in Saudi Arabia Electronic Health Records[43]	2021	Hyperledger Fabric	Utilização blockchain para criar uma rede peer-to-peer para sistemas de saúde no reino da Arábia Saudita para armazenar registros de saúde eletrônicos com uso de contratos inteligentes.
Decentralized Secure Personal Health Record Monitoring System using Blockchain[44]	2021	Hyperledger Fabric	Gerenciamento de registros de saúde pessoal (PHR) usando contratos inteligentes.
The Application of Blockchain to Electronic Health Record Systems:A Review [45]	2021	Blockchain pública e privada	Revisão de pesquisas relacionadas a blockchain e à IoT, detalhando as funções do sistema de prontuário eletrônico na área de saúde e médica.
Digital Healthcare using Blockchain [46]	2022	Blockchain Ethereum	Problemas e soluções no armazenamento digital de dados de saúde usando blockchain.
An Electronic Health Record Management System Based on Blockchain Technology [47]	2022	Blockchain Ethereum	Sistema de EHR com acessibilidade de informações através de Contratos inteligentes.

Na tabela 1: Artigos relacionando Blockchain e Healthcare de 2016 a 2022.

Fonte: Autor, 2023.

A utilização da blockchain tem simplificado significativamente o gerenciamento dos cuidados centrados no paciente, uma vez que permite que os pacientes assumam o controle de seus próprios dados médicos. Muitas vezes, os pacientes sentem frustração devido à repetição de processos de entrada de dados em diferentes sistemas de saúde, o que pode levar a inconsistências e dificuldades na comunicação entre os prestadores de cuidados de saúde. Uma solução promissora para esse desafio é a implementação de uma blockchain controlada pelo paciente para verificação de identidade e compartilhamento seguro de informações médicas.

Essa blockchain, especificamente projetada para fins de saúde, permitiria que os pacientes armazenassem de forma segura e acessível informações médicas , como históricos de saúde, resultados de testes, prescrições e registros de tratamentos. Ao ter controle direto sobre seus próprios dados, os pacientes podem autorizar o acesso a profissionais de saúde e instituições específicas, garantindo que suas informações sejam precisas, completas e sempre atualizadas.

Para o ano de 2023, na tabela 2 a seguir, observa-se artigos relevantes da aplicação da blockchain na área médica, sobretudo com a utilização de Contratos Inteligentes.

2023		
MedEHR-Eletronic Health record using blockchain [48]	Blockchain Ethereum	Plataforma para armazenamento de dados médicos eletrônicos com uso de contratos inteligentes.
Significance of Blockchain Technology in the Healthcare Sector [49]	Blockchain privada	Segurança dos prontuários médicos eletrônicos dos pacientes utilizando contratos inteligentes.
Sharding-based scalability enhancement of blockchain-based health application [50]	Hyperledger Fabric	Gerenciamento de dados de saúde com abordagem em fragmentação de dados e escalabilidade.
An Electronic Health Record Management System Based on Blockchain Technology [51]	Hyperledger Fabric	Sistema para intercâmbio de dados entre organizações de saúde e fornecedores de aplicativos, com avaliação das vantagens e desvantagens dos sistemas EHR.
Digital Health Data Supervision using Blockchain in Ethereum Testnet [52]	Ganache da Ethereum	Gerenciamento centrado no paciente, controlando os dados por meio de contratos inteligentes.
Electronic Healthcare Management System using Blockchain Technology [53]	Ganache da Ethereum	Blockchain Ethereum autorizada para estabelecer uma conexão global entre hospitais e pacientes por meio EHR.

Tabela 2: Artigos relacionando Blockchain e Healthcare em 2023.

Fonte: Autor, 2023.

3 REFERENCIAL TEÓRICO

3.1 Funcionamento da Blockchain

A blockchain, é um livro contábil (livro-razão) onde são registradas transações na ordem cronológica, sem a necessidade de uma autoridade central e formando um histórico de todas as transações. É uma rede distribuída com registro compartilhado e imutável, facilitando transações e rastreamento de ativos como casa, dinheiro, propriedade intelectual, patentes ou marcas. Praticamente qualquer item de valor pode ser rastreado na blockchain [54].

As transações são registros da sequência de operações realizadas entre os clientes de um sistema, que pode ser a troca de um ativo. Cada transação é agrupada em um bloco, a unidade fundamental de armazenamento de dados na blockchain, e cada bloco é conectado ao bloco anterior, formando assim uma cadeia de blocos. Em português, a palavra “blockchain” é traduzida como “cadeia de blocos” [55].

Na figura 4, observa-se uma rede blockchain. No passo 1, solicita-se a transação; no passo 2, a transação é representada como um bloco; no passo 3, o bloco é replicado a todos os nós da rede; no passo 4, os nós validam a transação; no passo 5, o novo bloco é adicionado na cadeia de blocos existentes; e, no passo 6 a transação está completa.

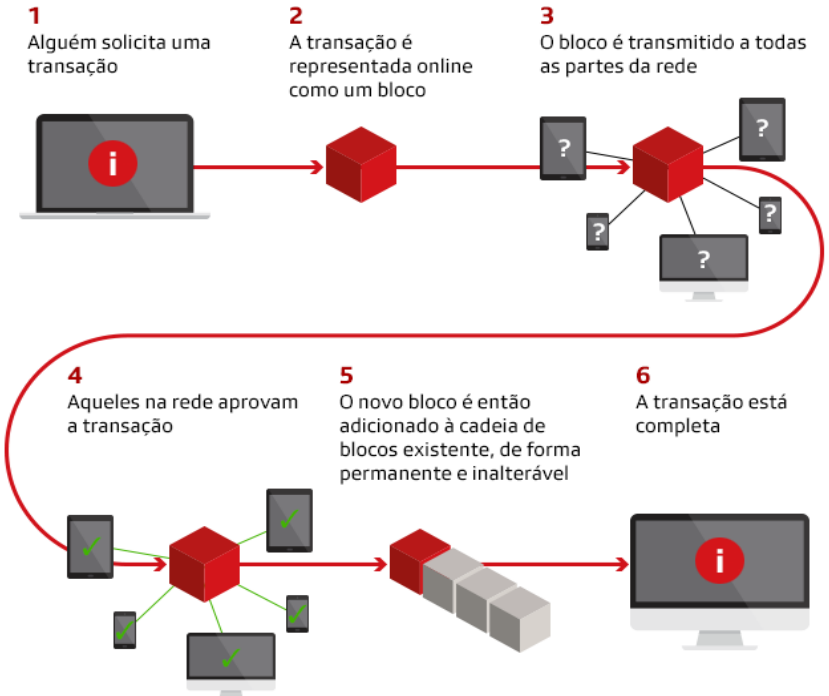

Figura 4: Funcionamento básico da Blockchain.

Fonte: Financial Times, 2020.

Cada bloco possui um cabeçalho e um corpo. O cabeçalho contém informações como, um identificador único (hash), o hash do bloco anterior (formando uma referência ao bloco anterior na cadeia), o nonce e outros metadados relevantes. O corpo do bloco contém as transações que foram incluídas no bloco, como transferências de criptomoedas, contratos inteligentes ou qualquer outro tipo de interação que possa ser registrada na blockchain. Esses blocos são distribuídos e mantidos por nós (computadores) que colaboram para validar e registrar as transações. O nonce é um valor que fica no cabeçalho, sendo adicionado na função para gerar o hash do bloco e, conectado aos demais atributos. Esse valor é incrementado até que se encontre um hash que represente o hash do bloco concatenado com bits zeros no início [55].

Cada bloco conectado ao bloco anterior, forma a cadeia na qual cada bloco da estrutura faz referência ao hash do bloco que o antecede. O valor hash do bloco anterior é utilizado para calcular o valor hash do bloco atual, criando assim a cadeia de dependência. Essa estrutura encadeada de blocos torna a blockchain imutável e resistente a qualquer tipo de alteração. Qualquer modificação em um bloco afetaria todos os blocos subsequentes na cadeia, exigindo o consenso da maioria da rede para ser aceita. Além disso, a criptografia utilizada na blockchain é extremamente robusta e requer uma quantidade significativa de tempo e energia para ser quebrada, o que adiciona outra camada de segurança à integridade da blockchain [56].

A existência de uma longa cadeia garante que uma vez que um bloco tenha várias gerações o sucedendo, ele não pode ser alterado sem recálculo de todos os blocos subsequentes. Isso requer uma quantidade significativa de poder computacional, tornando a blockchain imutável. Portanto, para fazer atualizações, um novo registro deve ser criado [55,56].

Essa estrutura se assemelha a uma lista encadeada, na qual cada bloco inclui um hash do bloco anterior em seu cabeçalho. O processo começa no bloco gênese (o único que não possui o hash do bloco anterior em seu cabeçalho), pois é o primeiro da cadeia, e continua até o bloco mais recente que possuem informações completas em seus cabeçalhos, ver figura 5.

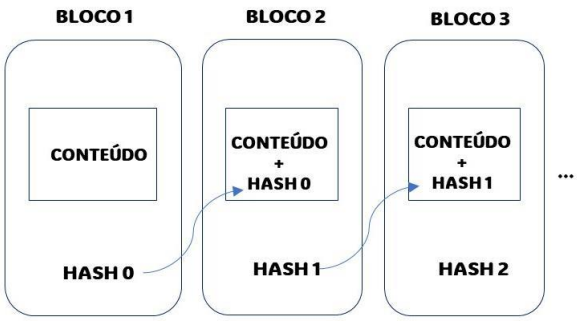

Figura 5: Encandeamento de blocos.

Fonte: Autor, 2023.

Cada usuário na rede possui um par de chaves: uma chave privada e uma chave pública. A chave privada é usada para gerar assinaturas digitais, garantindo que uma transação seja válida. A chave pública é derivada da chave privada usando algoritmos de criptografia assimétrica, e é compartilhada publicamente e serve como endereço para receber fundos. Um usuário cria uma transação com a chave pública do destinatário e a transação é então assinada com a chave privada do remetente. A chave pública do remetente também é incluída na transação para fins de verificação. A transação é transmitida aos nós para ser validada. Sendo validadas são agrupadas em blocos que são encadeados a blocos anteriores e o mineradores competem para resolver a prova de trabalho para ter o direito de adicionar o novo bloco resultante. Uma vez que novo o bloco é adicionado à blockchain, as transações são replicadas entre todos os nós que passam a ter uma cópia idêntica de todas as transações e tornam parte do histórico permanente. São chamados de mineradores os nós individuais que garantem a legitimidade da transação e o processo de criação de blocos é chamado mineração [55, 56].

3.2 Teoria do Bitcoin

O Bitcoin é um sistema de pagamentos eletrônicos de transações ponto a ponto e instantâneas, sem necessidade de um servidor central para processar as transações. Além disso, suporta desenvolvimento de protocolos de camada de aplicação, que combinam transações seguras com armazenamento e transferência de dados on-chain [57].

Aplicações que usam o Bitcoin para armazenar e recuperar dados estão surgindo em ritmo crescente. O Bitcoin atua como um servidor de carimbo de data/hora, permitindo que os dados sejam validados por meio de transações. São os opcodes que enviam dados arbitrários para as transações, instruções de baixo nível que definem operações que podem ser executadas no bitcoin script, a linguagem que especifica condições de gasto nas transações. Dessa forma, o Bitcoin é empregado como canal de transporte para as informações [56].

Os opcodes permitem a implementação de funcionalidades avançadas, como os contratos inteligentes e outras lógicas personalizadas. Cada cabeçalho contém um hash duplo SHA-256 (Secure Hash Algorithm) de uma árvore Merkle que agrupa as transações, um timestamp, o hash do bloco anterior, uma Prova de Trabalho, a versão do bloco, o nonce e outros metadados importantes [57].

A blockchain possibilita o rastreamento de todos os blocos até o bloco inicial. A cada 10 minutos, os mineradores criam um bloco, com o algoritmo de dificuldade ajustando-se para

manter essa taxa constante. Além disso, o consenso sobre a validade das transações é alcançado rapidamente, em questão de segundos. Isso é possível porque as transações são propagadas pela rede e verificadas pelos nós, e o consenso é alcançado quando a maioria dos nós concorda sobre a validade de uma transação ou de um novo bloco. Esse sistema torna a blockchain ágil e eficiente, permitindo transações rápidas e seguras [58].

No processo de transação, os satoshis (sats), a menor unidade de Bitcoin (1 BTC corresponde a 100.000.000 sats), contidos nas entradas das transação são combinados e gastos para criar um conjunto de "saídas de transação não gastas", também conhecidas como UTXOs (Unspent Transaction Outputs). Quando uma transação é feita, os UTXOs que são utilizados como entrada na transação, são consumidos, o que significa que eles são gastos na transação anterior para criar saídas de transação futuras [57].

Cada UTXO é protegido por um script de quebra-cabeça (script de desbloqueio) que define as condições sob as quais a UTXO pode ser gasto. Durante o processo de gasto, o script de quebra-cabeça resolvido correspondendo à UTXO, tem a solução como prova de que é o proprietário do UTXO e tem permissão para gastá-lo. A Prova de Trabalho é fundamentada no cálculo de hashes, competindo pelo privilégio de adicionar um novo bloco à cadeia. A Prova de Trabalho mais longa de cada bloco é incluída no bloco subsequente, formando assim a estrutura da cadeia e a solução para o quebra-cabeça do script é registrada na transação [55,56].

Existem três elementos primitivos encontrados no Bitcoin, a serem vistos: Funções Hash, Assinaturas Digitais e Árvores Merkle.

3.2.1 Funções de Hash

O Bitcoin utiliza duas funções hash: SHA-256 e RIPEMD-160 (Race Integrity Primitives Evaluation Message Digest) de 160 bits. São funções amplamente utilizadas em aplicações de segurança e criptografia, com algoritmos matemáticos que mapeiam dados de qualquer tamanho para uma cadeia de bits de tamanho fixo. Recebem uma mensagem arbitrária m e produz um valor h = H(m) de tamanho fixo. O SHA 256, resulta em uma string de 32 bytes que tornam efetivamente impossível reverter a saída, pois a função é unidirecional [57] .

O cabeçalho do bloco é identificável por um hash gerado usando o algoritmo de hash criptográfico SHA256. O hash SHA-256 deve ser menor ou igual ao alvo atual para que o bloco seja aceito pela rede. Quanto menor o alvo, mais difícil será gerar um bloco. O alvo é um número de 256 bits (extremamente grande) compartilhado por todos os clientes Bitcoin. Cada hash basicamente fornece um número aleatório entre 0 e o valor máximo de um número de 256

bits. As funções de hash são essenciais para a busca eficaz de dados, empregadas na pesquisa e recuperação eficiente de informações em grandes conjuntos de dados, são mecanismos de indexação eficientes. Devido à impossibilidade de regenerar os dados originais a partir do valor de hash, são cruciais para a segurança e a proteção da privacidade [58].

O RIPEMD-160 é uma função hash criptográfica baseada na construção Merkle – Damgård, produz um hash de 160 bits, o que o torna útil em aplicações onde um tamanho de hash menor é necessário. Essa construção é um método comum para construir funções hash criptográficas a partir de funções de compressão de bloco fixo [59].

3.2.2 Assinatura Digitais

São técnicas criptográfica que provam a autenticidade e integridade de uma mensagem eletrônica, obtendo-se um código único para utilizá-lo como assinatura. Na composição da assinatura utiliza-se da criptografia de chave pública para criptografar um valor hash e assinar documentos digitalmente entre duas pontas. Desse modo, um cliente utiliza da chave privada para assinar o documento e outro utiliza-se da chave pública para fazer a leitura. Alguns Protocolos de Assinatura Digital são: RSA (Rivest-Shamir-Adleman); EdDSA (Edwards-curve Digital Signature Algorithm); HMAC (Hash-based Message Authentication Code). Além dos protocolos ECDSA e DAS que são especificados abaixo [60]:

- ECDSA (Elliptic Curve Digital Signature Algorithm): É um algoritmo de assinatura baseado em curvas elípticas. Oferece a mesma segurança que o RSA, mas com tamanhos de chave menores, e é mais eficiente em termos de recursos.
- DSA (Digital Signature Algorithm): O DSA é um protocolo de assinatura digital amplamente utilizado em criptografia de chave pública. É frequentemente usado em conjunto com o algoritmo Diffie-Hellman para garantir autenticidade e integridade.

O ECDSA, algoritmo de chave assimétrica, utiliza um par de chaves, uma privada e uma pública. A geração de números aleatórios é crucial na criação da assinatura e o algoritmo usado deve ser conhecido e confiável. O SHA-256 é um algoritmo usado com ECDSA. Uma assinatura ECDSA é criada usando uma chave privada e um hash da mensagem assinada e para verificar a assinatura, é necessário a chave pública correspondente à privada usada na criação. A chave privada deve ser armazenada de forma segura para evitar acesso não autorizado. São assinaturas codificadas usando o formato Distinguished Encoding Rules (DER) [59, 60].

3.2.3 Árvores Merkle

Uma árvore de Merkle é uma estrutura na qual as folhas representam os dados e os nós internos são valores de hash gerados a partir das folhas. A raiz da árvore é, portanto, o hash de todos os dados contidos nas folhas. Essa abordagem tem a capacidade de fornecer uma prova de integridade eficiente, conhecida como "Prova de Merkle", que verifica se determinado bloco faz parte da árvore de maneira eficaz, reduzindo a complexidade para logarítmica (log(n)) [61].

Isso significa que para provar que uma folha pertence à árvore, é necessário fornecer apenas os hashes dos nós adjacentes na árvore, em vez de toda a estrutura. Cada nó interno de uma árvore Merkle é calculado a partir do hash dos seus nós filhos. Portanto, se você tem o hash dos nós filhos, pode reconstruir facilmente o hash do nó pai. Para provar que o bloco 000 pertence à árvore Merkle, basta fornecer o hash do bloco 001 (nó adjacente) e o hash 1 (nó pai do bloco 001), conforme ilustrado na figura 6 [61].

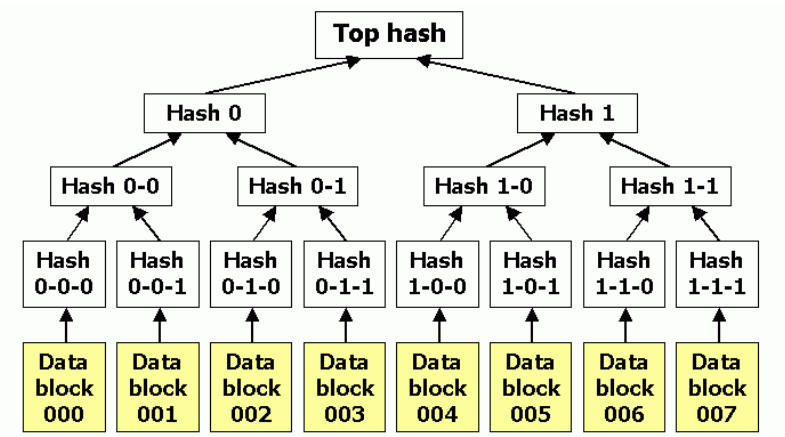

Figura 6: Árvore de Merkle.
Fonte: GTA/UFRJ, 2018.

3.3 Algoritmo de consenso

Os protocolos de consenso são aplicados a sistemas computacionais distribuídos e fundamentados no problema da confiança entre os pares da rede. No Bitcoin, é utilizado o algoritmo de consenso bizantino tolerante a falhas que utiliza o conceito de Prova de Trabalho e incentivos econômicos para gerenciar direitos de tomada de decisão, referido como o consenso de Nakamoto, conforme definido no seu whitepaper, onde os nós votam para fazer cumprir as regras usadas para construir os blocos que compõem o livro-razão do Bitcoin [62].

O consenso de Nakamoto define um nó honesto como aquele que busca a cadeia de blocos válida mais longa e aplica prova de trabalho para estender essa cadeia. Neste contexto,

a cadeia mais longa representa a maior prova de esforço de trabalho na cadeia válida. Se a maioria dos nós for honesta, então a cadeia honesta crescerá com a maior prova de trabalho e ultrapassará quaisquer outras cadeias concorrentes. Ao escolher em qual cadeia construir, os nós votam para fazer cumprir as regras que regem o protocolo e usam o Blockchain como um livro-razão financeiro global com supervisão legal e regulatória. Através do consenso de Nakamoto, a prova de trabalho na cadeia mais longa torna-se uma barreira econômica e técnica a ser ultrapassada por qualquer atacante. Ao mesmo tempo, a recompensa do bloco como incentivo econômico leva o nó a seguir o consenso, incentivando a honestidade e a cooperação entre os mineradores concorrentes [63].

O Bitcoin utiliza o algoritmo de prova de trabalho denominado PoW (Proof of Work) para validar e aceitar os blocos. O esquema de prova de trabalho é baseado no Hashcash e utiliza o algoritmo de hash SHA-256. Através da prova de trabalho, os mineradores competem para resolver um problema matemático complexo, que envolve encontrar um valor hash que atenda a determinados critérios. Esse processo de mineração, envolve tentativas computacionais intensivas para solucionar o problema e o nó que resolve primeiro ganha o direito de adicionar o bloco à rede e recebe uma recompensa, além disso, os mineradores também cobram taxas de transação, o que os incentiva ainda mais a proteger a rede. O consenso ocorre por meio da escolha da cadeia mais longa como sendo a verdadeira [63].

O poder computacional significativo exigido, é o que torna a rede Bitcoin segura e resistente à ataques. A prova de trabalho, torna a rede segura contra fraudes, pois a maioria dos mineradores precisa confirmar a autenticidade de cada bloco antes de adicioná-lo a blockchain. O algoritmo PoW, inicialmente proposto por Adam Back, tem como ideia desmotivar ataques cibernéticos. Para atingir este objetivo, deve-se por meio da prova de trabalho provar que gastou certo tempo para encontrar a resposta. A tarefa de encontrar a resposta é baseada em dois princípios: a prova de trabalho tem que ser difícil e trabalhosa, mas não impossível; e a verificação da prova deve ser rápida e fácil [63].

A tarefa de criar blocos é controlada ajustando a dificuldade, garantindo que um novo bloco seja adicionado a cada 10 minutos. Para ser válido, um bloco deve ter um valor de hash menor que ao alvo atual, indicando que o trabalho foi realizado. Cada bloco contém o hash do bloco anterior, e alterar um bloco exigiria recriar todos os blocos subsequentes. Isso mantém a segurança, a integridade da cadeia contra adulteração e a estabilidade da rede [63].

3.4 Redes Peer To Peer e a Rede Bitcoin

Uma rede peer-to-peer (P2P), é uma arquitetura de sistemas de computação distribuída, de maneira que as máquinas cooperem entre si, exercendo os papéis de cliente e servidor, eliminando a necessidade de uma autoridade central. Em redes P2P, um nó é um dispositivo ou entidade que participa da rede, como mostrado na figura 7. É uma das tecnologias usadas para que as redes blockchain possam funcionar, criando rede de comunicação de dados distribuída e protegida criptograficamente [64].

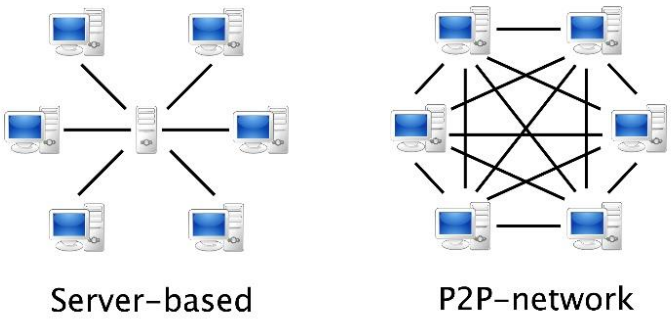

Figura 7: Arquiteturas servidor e P2P.
Fonte: SQL Data, 2019.

Cada nó pode agir como um ponto de origem, destino ou de trânsito para comunicações dentro da rede. Os nós de uma rede P2P trabalham juntos para formar uma infraestrutura distribuída e descentralizada, onde não há uma autoridade central controlando a rede, mas sim uma rede de nós que colaboram entre si para alcançar os objetivos da rede [64].

Os nós, frequentemente chamados de mineradores, têm a capacidade de construir, distribuir e validar os blocos. Eles mantêm o mecanismo de consenso baseado na distribuição de blocos e na prova de trabalho, além de validar e propagar transações. As transações são inseridas na rede pelos usuários, que interagem com os nós Bitcoin. Os usuários podem ser provedores de serviços, entidades de armazenamento, contratos inteligentes ou carteiras de pessoas ou empresas. Um nó Bitcoin não precisa ser uma única máquina, pode ser composto por vários sistemas interligados, como roteadores ou bancos de dados [64].

3.5 Blockchain Bitcoin

O Bitcoin foi inicialmente delineada por Satoshi Nakamoto no white paper intitulado "Bitcoin: A Peer to Peer Electronic Cash System" em 2008. O Bitcoin (BTC) criado por Satoshi Nakamoto, foi a criptomoeda pioneira da blockchain. Surge em 2017, o Bitcoin Cash (BCH) como uma bifurcação do BTC, devido a discordâncias sobre o tamanho dos blocos. O BCH aumentou o tamanho dos blocos para permitir transações mais rápidas e econômicas. No entanto, isso gerou controvérsias, pois alguns acreditavam que quebraria o protocolo original de Nakamoto. A disputa resultou no "hard fork" que deu origem ao BCH, que ampliou o limite do bloco para 8 MB e, atualmente podem chegar a 32 MB, enquanto o Bitcoin tinha limitado os blocos a 1 MB [65].

Em 2018 surgiu uma nova criptomoeda, o BSV (Bitcoin Satoshi Vision), uma bifurcação do Bitcoin Cash (BCH), visando restaurar o protocolo original de Nakamoto, enfatizando a escalabilidade ao aumentar o tamanho do bloco para 128 MB e, portanto, o número de transações que podem ser confirmadas em um único bloco. Além disso, havia planos para aumentar o tamanho do bloco para 2 GB, que mais tarde foi aumentado para 4 GB. Em 2018, o BSV torna-se o novo símbolo do Bitcoin original, procurando preservar a essência do protocolo e aumentando a capacidade da atividade onchain, enquanto o BCH se desviou do white paper do Bitcoin, introduzindo recursos não compatíveis com o Bitcoin [65, 66].

Em 4 de fevereiro de 2020, o Bitcoin SV passou por um hard fork denominado "Genesis", que restaurou o protocolo original do Bitcoin. Removeu-se o limite máximo padrão para o tamanho dos blocos e reverteu-se as alterações feitas pelos desenvolvedores ao longo da evolução do Bitcoin. O objetivo principal era retornar o protocolo para a visão original de Satoshi. Portanto, o BSV posiciona-se como a verdadeira visão de Satoshi Nakamoto [66]

O dimensionamento ilimitado e a linguagem de script com Bitcoin original permitem desenvolvimento de aplicativos com mais facilidade e escalabilidade. Em 2021, o BSV demonstrou um rendimento de 50K transações por segundo, a um custo baixo e extraiu os primeiros blocos a nível de GB (1GB), atingindo até 2 GB em agosto de 2021. Atualmente, com o aumento do bloco para 4 GB, a criptomoeda visa continuar aumentando a capacidade de processamento de transações e com taxas reduzidas. Além disso, o BSV se destaca entre a mais amigável às empresas, permitindo aplicativos em grande escala e suportando soluções empresariais complexas, incluindo aquelas que lidam com grandes volumes de dados [66,67].

O número recorde de transações só é possível no BSV, pois é o único protocolo que pode atingir um bilhão de transações por segundo (TPS). Em 26 de outubro de 2023, a plataforma quebrou o recorde mundial de prova de trabalho com mais de 91 milhões de transações em 24h, observa-se na figura 8. Anteriormente, em 8 de agosto de 2023, em um período de 24h, o recorde foi de 128,691 milhões de transações on-chain. Em testes, o Teranode da BSV produziu em março de 2024, blocos com mais de 1 TBytes de TPS [66, 67, 68].

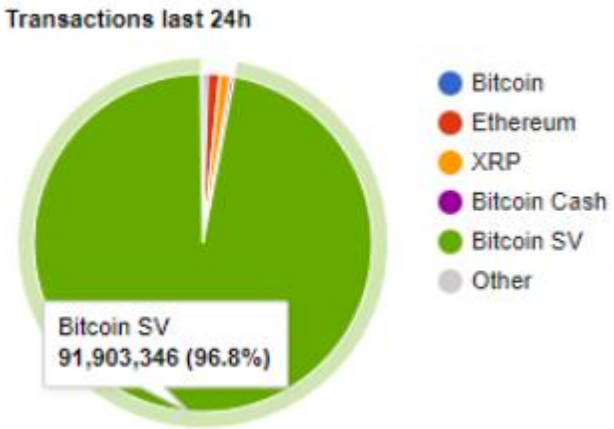

Figura 8: Recorde de transações em 24 horas em 26 de outubro de 2023.

Fonte: Jon Southurst, 2023.

Na tabela 3, observa-se diversos fatores para se considerar a escalabilidade de uma blockchain, além do tamanho do bloco, a escalabilidade está ligada a quantidade de transações que a rede é capaz de processar em um determinado período, entre outras características.

PLATAFORMAS	T.P.S	B.S	ALGORITMO	FEE RATE	DADOS ON CHAIN
ETH	21 TPS	126 KB	POS	Muita alta	não
Hyperledger	3K TPS	-	POET	-	não
BTC	7 TPS	4 MB	POW	Muita alta	não
BSV	11, 887 -50K TPS	4 GB	POW	Baixa	sim
Solana	650K TPS	128 MB	POW	Baixa	não
TON	104K TPS	N/A	POS-sharding	Baixa	não

Tabela 3: Comparativo das tecnologias Blockchain.

Fonte: Autor, 2024.

3. 6 Ethereum e Smart Contracts

Após o lançamento do BTC, ficou evidente que a tecnologia blockchain tinha aplicações além das moedas digitais. O primeiro grande projeto após o Bitcoin, foi a plataforma Ethereum, lançado em 2015 por Vitalik Buterin, um programador russo-canadense. A nova blockchain, concebida como uma criptomoeda baseada nos princípios do Bitcoin, trouxe a inovação de criar Smart Contracts (Contratos Inteligentes), programas altamente versáteis que executam automaticamente acordos com regras predefinidas, sem a necessidade de um intermediário de confiança [69].

A plataforma Ethereum introduziu a capacidade de criar contratos inteligentes complexos usando a Ethereum Virtual Machine (EVM), que é Turing-completa, isso a torna flexível e adequada para uma variedade de protocolos financeiros e não financeiros. Enquanto o Bitcoin se concentrava em transações confiáveis e descentralizadas, o Ethereum foi projetado para facilitar transações de todos os tipos sem intermediário, superando barreiras como sistemas legais ineficientes, distâncias geográficas e corrupção [69, 70].

Na Ethereum, os contratos são executados exigindo uma taxa chamada de "Gás", um mecanismo de proteção que evita consumo infinito de recursos por engano ou por atos maliciosos, garantindo uma taxa limitada para evitar loops infinitos e impedir o travamento da rede. Foi projetada para ser uma Proof of Stake, mas a tecnologia não estava pronta para promover essa migração e foi implementado um mecanismo interno denominado bomba de dificuldade que aumenta a dificuldade de mineração [70].

Comparativamente, o Bitcoin é um sistema de transição de estado, onde o estado consiste no status de propriedade dos bitcoins existentes e a função de transição de estado gera um novo estado, a partir de um estado existente e uma transação. O estado é a coleção de todas as UTXOs. Uma transação contém uma ou mais entradas, com cada entrada contendo uma referência a um UTXO existente e uma assinatura criptográfica produzida pela chave privada associada ao endereço do proprietário, e uma ou mais saídas, com cada saída contendo um novo UTXO a ser adicionado ao estado [69].

O Bitcoin promove descentralização através do consenso, onde os nós competem para criar blocos de transações, garantindo escalabilidade e armazenando dados em sua estrutura multinível. Essa arquitetura contribui para a segurança e eficiência do sistema. Permite adoção de contratos inteligentes usando scripts para vincular a UTXOs a condições específicas. No entanto, a linguagem de script no Bitcoin foi caracterizada por anos com limitações de falta de completude de Turing, o que resultou em scripts considerados ineficientes [69].

O white paper BitVM de 9 de outubro de 2023, intitulado como “BitVM: Compute Anything on Bitcoin” baseado na arquitetura de Robin Linus, incorpora provas de fraudes e avanços recentes na árvore de Merkle, oferecendo uma nova maneira de implantar contratos inteligentes Turing completos na rede Bitcoin sem alterar regras de consenso da rede, contrariando que Vitalik Buterin disse a respeito do bitcoin em 2014 em seu white paper [71].

Com o BitVM, a lógica dos contratos do Bitcoin é executada off-chain, mas a verificação é realizada na própria rede do Bitcoin. Isso possibilita a implementação de contratos inteligentes mais avançados na rede Bitcoin, mantendo sua integridade e segurança. Um sistema Turing Completo, teoricamente capaz de resolver qualquer problema computacional, agora definitivamente demonstrado através do white paper BitVM [71].

O termo “Smart Contract” é muito anterior ao Bitcoin, foi em 1994 que o cientista de computação e criptógrafo Nick Szabo introduziu o termo, e idealizou a representação digital de contratos tradicionais, com minimização da necessidade de confiança em intermediários, definindo os contratos como: “A smart contract is a computerized transaction protocol that executes the terms of a contract.” São escritos em linguagem de programação, e nada mais são do que um conjunto de código, que seguem a lógica if-this-then-that, ou seja, quando algum evento acontece, ele desencadeia uma reação. Szabo enfrentou desafios ao idealizá-los. Para que funcionassem, eles precisariam buscar e armazenar informações em registros, que antes nos bancos de dados tradicionais eram suscetíveis à manipulação centralizada. No entanto, com a blockchain, possibilitou-se contratos em registros distribuídos e imutáveis [72, 73, 74].

Esses contratos, são contratos jurídicos digitais que automatizam a execução de instruções, assegurando conformidade com os termos contratuais quando condições são atendidas. A blockchain aumenta a segurança e transparência nas transações, eliminando falsificações e intermediários, pois as transações tornam-se descentralizadas [73,74].

Com a ideia de Vitalik publicando o whitepaper do Ethereum em novembro de 2013 e unindo a ideia de Smart Contracts de Nick Sazbo mais a tecnologia de Satoshi Nakamoto, o Ethereum, se tornou a primeira plataforma para criação de Smart Contracts, com seu lançamento em 2015. A solução de Nick Szabo aprimorada por Vitalik Buterin, proporciona velocidade e segurança na execução de termos contratuais, graças à criptografia e ao registro na blockchain, prevenindo alterações não autorizadas [72,74].

Os contratos inteligentes desempenham um papel crucial no ecossistema blockchain, oferecendo uma forma transparente e segura de realizar transações sem intermediários. Diversas indústrias estão explorando seu potencial, incluindo finanças, imóveis, cadeia de abastecimento,

saúde e setor jurídico, entre outros. Na área da saúde, eles automatizam processos como a manutenção de registros médicos, e diversas outras aplicações, reduzindo custos, aumentando eficiência e aprimorando a privacidade e segurança dos pacientes [75].

Na Bitcoin SV, os contratos inteligentes são implementados usando a linguagem de script do Bitcoin, para definir condições e lógica de execução, sendo possível desenvolver uma variedade de contratos inteligentes, incluindo contratos de transferência condicional, contratos de votação, contratos de tokenização e muito mais. Para a implementação, os desenvolvedores podem usar frameworks e ferramentas específicos. Além disso, a BSV tem explorado várias soluções de escalabilidade e aumento de capacidade para garantir que os Smart contracts possam funcionar de forma eficiente em sua blockchain [76].

3.7 Smart Contracts na Blockchain BSV

A framework que os desenvolvedores utilizam para a escrita de contratos inteligentes no Bitcoin, é o sCrypt, uma framework em TypeScript, uma linguagem de programação de alto nível que compila para script bitcoin, a linguagem nativa do Bitcoin. Ela fornece uma abstração mais amigável ao desenvolvedor em relação ao script bitcoin [76].

Os opcodes (códigos de operação, comandos ou funções) são uma lista de todas as palavras do bitcoin script. São instruções de baixo nível que definem as operações que podem ser executadas no bitcoin script. São os opcodes que enviam dados arbitrários para as transações. O Bitcoin script, é a linguagem que especifica condições de gasto nas transações, dessa forma o Bitcoin é empregado como canal de transporte para as informações [56, 77].

Cada opcode executa uma operação específica no bitcoin script. Os opcodes podem ser utilizados para criar condições de gasto personalizadas nas transações, permitindo a implementação de funcionalidades avançadas, como contratos inteligentes, transações multisig (que exigem várias assinaturas para serem gastos), e outras lógicas personalizadas [77].

Alguns exemplos de opcodes incluem:

1. OP_CHECKSIG: Verifica a assinatura digital de uma chave pública.
2. OP_EQUAL: Compara dois valores para igualdade.
3. OP_HASH160: Realiza o hash SHA-256 seguido de RIPEMD-160 em uma sequência de dados.
4. OP_IF: Executa uma operação condicional.
5. OP_RETURN: Marca a saída da transação como inválida e pode ser utilizada para armazenar dados na blockchain de forma não gasta.

Esses são apenas alguns exemplos e existem muitos outros opcodes disponíveis que permitem ampla gama de funcionalidades e flexibilidade na construção de transações Bitcoin.

A seguir na figura 9, um contrato inteligente popular no Bitcoin, o Pay to Public Key Hash (P2PKH) em TypeScript. Nesse tipo de contrato, os fundos são bloqueados em uma transação que só pode ser desbloqueada pelo proprietário da chave privada correspondente ao hash da chave pública. O endereço para o qual os fundos são enviados não é diretamente a chave pública do destinatário, mas sim um hash dessa chave pública [76].

```
export class P2PKH extends SmartContract {
    @prop()
    readonly address: Addr

    constructor(address: Addr) {
        super(..arguments)
        this.address = address
    }

    @method()
    public unlock(sig: Sig, pubkey: PubKey) {
        // make sure the `pubkey` is the one locked with its address in the constructor
        assert(pubKey2Addr(pubkey) == this.address, 'address check failed')

       // make sure the `sig` is signed by the private key corresponding to the `pubkey`
        assert(this.checkSig(sig, pubkey), 'signature check failed')
    }
}
```

Figura 9: Smart Contracts Pay to Public Key Hash (P2PKH).

Fonte: sCrypt, 2023.

Quando alguém quer enviar fundos para outro participante na rede, é criada uma transação que bloqueia esses fundos para um endereço gerado a partir do hash da chave pública do destinatário. Esse endereço é o que chamamos de “Pay to Public Key Hash”. O destinatário pode então desbloquear esses fundos, fornecendo a chave pública e uma assinatura válida na transação de desbloqueio. O contrato inteligente associado a esse tipo de endereço verifica se a chave pública fornecida corresponde ao hash armazenado no endereço. Se corresponder, a transação é considerada válida e os fundos são desbloqueados. Essa abordagem fornece uma camada adicional de segurança e privacidade, já que o endereço usado para receber os fundos não revela diretamente a chave pública do destinatário, mas apenas um hash dela. Isso garante que apenas o proprietário da chave privada possa gastar os fundos [78].

4 MATERIAIS E MÉTODOS

Primeiramente, foi realizado um levantamento na literatura para encontrar trabalhos semelhantes, bem como um estudo dos principais conceitos que evolvem o tema pesquisado. Para descrever a metodologia empregada, foram seguidas as seguintes etapas:

1. Revisão da Literatura;
2. Referencial Teórico;
3. Seleção do modelo de rede Blockchain;
4. Seleção do protocolo de consenso;
5. Seleção da Framework.

Na revisão da literatura, todos os trabalhos relacionados descreviam soluções com Smart Contracts na rede Ethereum. Esta dissertação, apresenta-se como inovadora em aplicação de Smart Contracts no gerenciamento de dados de saúde de um paciente na rede Bitcoin. Os diversos trabalhos relacionados abordaram o gerenciamento de registros eletrônicos com ênfase no uso da tecnologia Blockchain para conceder aos pacientes autonomia sobre a posse de seus próprios dados, seguindo a mesma ideia dessa proposta de dissertação. Destacou-se nesta revisão, a relevância do uso da tecnologia aplicada ao setor da saúde, demonstrando os desafios e o potencial dessa tecnologia a ser explorado no setor, além dos casos de sucesso ao redor do mundo, com aplicações do ano de 2016 a 2023.

O Referencial Teórico abordou o funcionamento básico da Blockchain e a teoria do Bitcoin, destacando aspectos técnicos que compõe a essência da tecnologia, como: Funções de Hash, Assinatura Digitais e Árvores de Merkle. Conceitos de arquitetura de computação, como protocolo de consenso e redes peer-to-peer e Smart Contracts.

Na metodologia proposta para este trabalho, optou-se por utilizar o modelo da rede Blockchain BSV. Essa rede tem sido reconhecida por explorar diversas soluções para escalabilidade e aumento da capacidade de gerenciamento de grandes volumes de dados. Na área da saúde, em particular, a BSV tem sido adotada, comprometendo-se com a privacidade e segurança dos dados dos pacientes. Destaca-se também como uma das mais amigáveis às empresas, permitindo a implementação de aplicativos em grande escala e suportando soluções empresariais complexas. É o modelo UTXO da rede BSV altamente descentralizado e flexível para o armazenamento de transações, que possibilita escalabilidade massiva, gerando confiança na capacidade da rede para lidar com volumes de transações de aplicativos robustos.

O protocolo de consenso é necessário por se tratar de uma estrutura descentralizada, é indispensável a confiança entre os pares, logo, são aplicados os protocolos de consenso para estabelecer confiança na validação dos blocos que serão adicionados na cadeia. O protocolo de Prova de trabalho (Proof-of-Work) é utilizado pelo Bitcoin e tem como principal característica a competição entre os nós para resolver problemas matemáticos complexos.

O framework escolhido para o desenvolvimento da aplicação e escrita de contratos inteligentes, é o sCrypt-TS, uma framework em linguagem TypeScript, criada para desenvolvedores Web3 na criação de aplicativos com tecnologia blockchain na rede BSV. Com o auxílio da ferramenta de desenvolvimento Visual Studio como suporte a linguagem TypeScript, compilando diretamente para o script bitcoin, é facilitado o desenvolvimento de contratos inteligentes na plataforma BSV. Portanto, é uma plataforma de desenvolvimento que facilita a interação entre o protocolo básico do Bitcoin e os desenvolvedores de aplicações, fornecendo assim uma camada de implementação.

Agora, apresenta-se um breve detalhamento da arquitetura proposta que visa obter um Sistema de Acesso e Compartilhamento de Dados de Saúde, especificamente usando para este teste piloto, imagens médicas.

O sistema proposto, conterá informações armazenadas na rede blockchain, disponíveis para um indivíduo específico por meio dos Smart Contracts, permitindo que os pacientes compartilhem suas informações com organizações de saúde e outros que desejar. Na figura 10, demonstra-se os componentes políticos e técnicos necessários para a uma interoperabilidade.

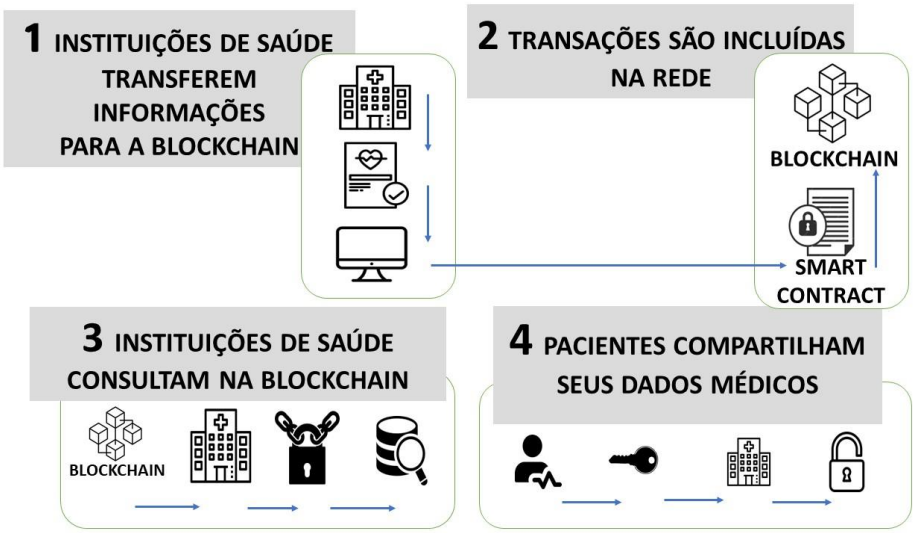

Figura 10: Arquitetura do Sistema de Acesso e Compartilhamento de Imagens.
Fonte: Autor, 2023.

A figura acima, apresenta a arquitetura que pode ajudar a criar um ecossistema a atingir metas de interoperabilidade. A estrutura da rede médica como na Figura 10, é descrita em: (1) Infraestrutura de rede médica que possui os dados de registros médicos (2) Identidade e autenticação dos usuários (paciente ou pessoa autorizada), (3) Pedido para acessar informações eletrônicas de saúde (4) Desbloqueio e acesso aos registros.

Portanto, a estrutura proposta possui três camadas e as diferentes comunicações entre os componentes é mostrado na Figura 11.

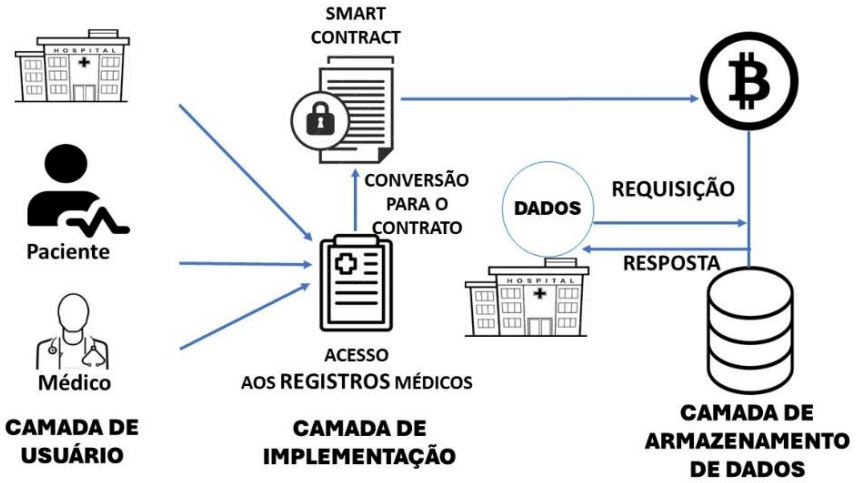

Figura 11: Camadas do sistema proposto.
Fonte: Autor, 2023.

As camadas são: camada de usuário, camada de implementação e camada de armazenamento de dados.

Camada do usuário: podendo ser composta por prontuário eletrônicos ou exames de imagens (radiologia, ressonâncias, ultrassonografias e tomografias). Essa camada verifica a identidade do usuário (paciente ou pessoa autorizada).

Camada de armazenamento de dados: A rede blockchain poderá armazenar os dados relacionados à saúde, prontuários eletrônicos, exames de imagem e outros.

Camada de implementação: Nesta camada acontece a implementação, com a escrita do código e execução do Smart Contracts. Por meio desses contratos - que são executados automaticamente quando as condições são atendidas - é verificada a identidade do usuário e se atendida as condições, desbloqueia-se o acesso das informações requisitadas. Temos o processo de acesso das informações armazenadas mediante a satisfação das condições estabelecidas no contrato. Utilizar-se-á a linguagem de programação typescript para desenvolver os contratos, definindo lógicas de permissões específicas para diferentes partes interessadas.

Observa - se na figura 12, o fluxograma do Smart Contract.

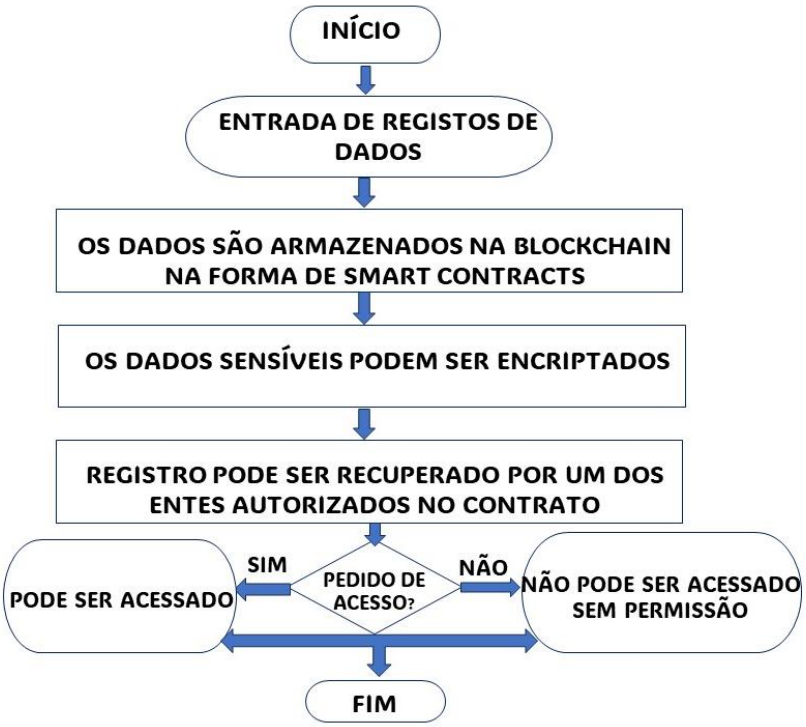

Figura 12: Fluxograma do Smart Contracts.
Fonte: Autor, 2023.

A blockchain BSV oferece a capacidade de armazenar diversos tipos de dados, fornecendo uma base sólida para a construção de aplicativos. Com transações imutáveis e um protocolo definido, possibilita na área de saúde, ser usada como uma camada segura para compartilhamento de dados padronizados entre organizações.

Após essas informações padronizadas serem definidas, contratos inteligentes são empregados para aplicar regras específicas ao processamento e armazenamento dessas informações na blockchain. Em cada interação com o paciente, as organizações de saúde enviam informações para um contrato inteligente, que verifica se os dados são válidos de acordo com os parâmetros estabelecidos. Quando o contrato inteligente valida os dados corretos, a transação é direcionada para armazenamento na blockchain.

4.1 Smart Contracts

Os contratos inteligentes partem da ideia de propriedades inteligentes para a blockchain, possibilitando desenvolvimento de aplicações a fim de automatizar a execução de transações e lógica de negócios em uma rede blockchain. Fornecendo uma camada de automação, segurança e transparência para transações e processos de negócios.

Comparando a rede Ethereum, pioneira e amplamente adotada na criação de contratos inteligentes, é fundamental compreender que cada uma possui suas vantagens e características distintas. A plataforma sCrypt da rede Bitcoin, vê-se nas figuras 13 e 14, desponta como a mais viável para a criação de contratos complexos.

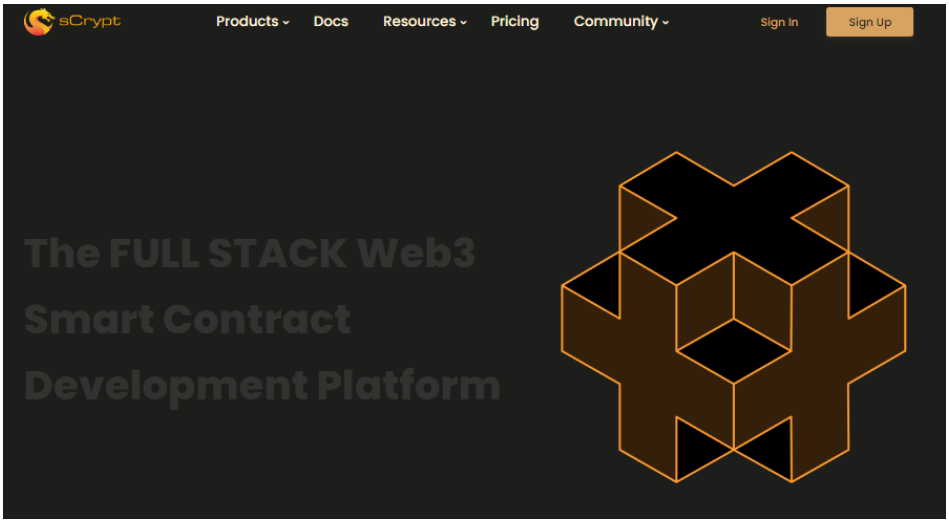

Figura 13: Plataforma sCrypt.
Fonte: Autor, 2023

Figura 14: Estrutura TypeScript para contratos inteligentes.
Fonte: Autor, 2023.

A plataforma sCrypt-TS, para programadores Web3 utilizando TypeScript, possibilita a criação de aplicativos na rede Bitcoin, com interação entre o protocolo bitcoin e os desenvolvedores de aplicativos, fornecendo uma camada de implementação acessível, demonstrando escalabilidade e oferecendo implementações para diversas aplicações.

4.2 Sistema UTXO

A implementação requer a seleção de um protocolo, ou seja, a estrutura que orienta o desenvolvimento da aplicação. A escolha do protocolo influencia na gama de aplicações e no número de usuários que participam da rede. Neste trabalho foi escolhida a rede BSV do Bitcoin e plataforma de desenvolvimento de contratos inteligentes sCrypt-TS.

O protocolo bitcoin é altamente descentralizado e flexível para o armazenamento de transações, com capacidade da rede para lidar com grandes volumes de transações. Os protocolos são conjuntos de regras armazenadas em transações como dados arbitrários, possibilitando implementações com funcionalidades para diversos casos de uso [79, 80].

O Bitcoin é um sistema de transição de estado, onde cada transação atualiza o estado existente. O estado é representado pela coleção de todas as moedas não gastas (UTXO - Unspent Transaction Output) [81]. Os UTXOs são gastos de forma independente, simplificando os mecanismos de validação, já que os nós só precisam verificar se os UTXOs gastos correspondem aos requisitos de entrada da transação, resultando em processos de validação mais simples e eficientes. Isso aumenta a escalabilidade e reduz os tempos de confirmação de transações, permitindo maior paralelismo no processamento de transações. Além disso, eles permitem a construção e assinatura offline de transações, o que pode ser útil em cenários com conectividade limitada à Internet [79].

O "estado" refere-se ao status atual de todas as contas, saldos, dados de contratos inteligentes e outras informações relevantes num determinado momento. É atualizado a cada nova transação, e pode ocorrer inchaço do estado, quando o tamanho dos dados acumulados se tornam impraticáveis para gerenciar com eficiência e consomem muitos recursos. Acontece à medida que mais transações são adicionadas, resultando numa quantidade crescente de dados que precisam ser armazenados e processados, incluindo nós completos. Os sistemas UTXO podem experimentar menos inchaço de estado, pois os UTXOs gastos são simplesmente removidos da razão, levando a um estado menor e mais eficiente [79,81].

4.3 Integração Back-end do Smart Contracts e a Interface de Usuário

Os Smart Contracts permitem que os usuários tenham controle sobre seus dados de saúde. Eles podem definir as condições sob as quais seus dados podem ser acessados, compartilhados ou utilizados por terceiros, garantindo assim maior autonomia e poder de decisão sobre suas informações médicas.

A camada back-end gerencia a lógica de negócios do Smart Contracts, como verificar permissões de acesso e processar transações. A camada back-end se conecta à blockchain através API dos nós onde o contrato está implantado usando a biblioteca “scrypt-ts”.

O desenvolvimento front-end desempenha um papel crucial na criação de interfaces de usuário interativas. A biblioteca usada para estabelecer uma base para a aplicação web é o React.js. O servidor de aplicativos responsável por receber solicitações da interface do usuário, processá-las e interagir com a blockchain é tecnologia Node.js. A interface de usuário é uma página da web ou um aplicativo móvel onde os usuários podem fazer login e acessar os recursos oferecidos pelo Smart Contracts.

O sCrypt permite escrever contratos inteligentes na Bitcoin Virtual Machine (BVM) usando TypeScript. Um exemplo simples de código TypeScript para um Smart Contracts no sCrypt, vê-se na figura 15.

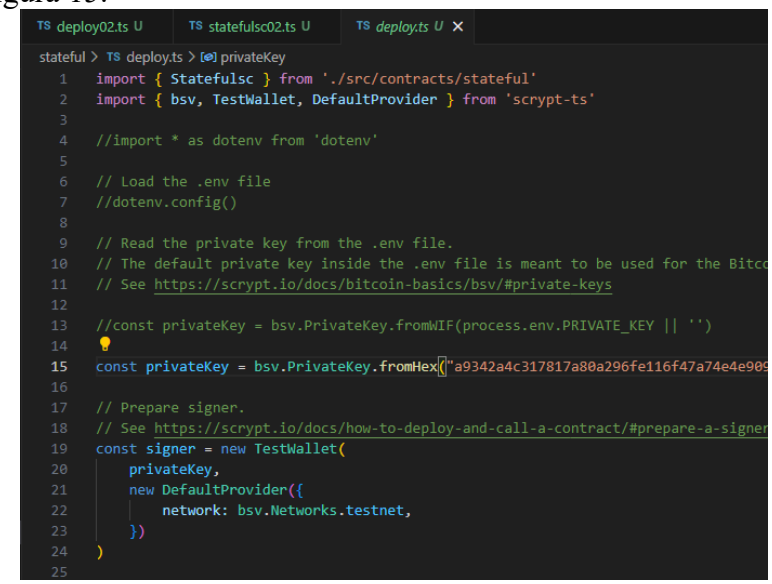

Figura 15: Código em TypeScript.

Fonte: Autor, 2024.

Também há os oráculos de Blockchain, que são cruciais para integrar informações do mundo real à blockchain, atuando como pontes entre esses dois domínios. Eles coletam, validam e fornecem dados externos à blockchain para uso em contratos inteligentes e outras aplicações na rede, superando a limitação da blockchain em acessar informações externas diretamente [76].

4.4 Padrão de Imagens DICOM

O padrão DICOM é amplamente utilizado para armazenar e transmitir imagens médicas, oferecendo estrutura padronizada que garante a compatibilidade entre diferentes

sistemas de imagem e equipamentos médicos. No entanto, a transferência de arquivos DICOM (Digital Imaging and Communications in Medicine) enfrenta desafios significativos em relação à segurança, privacidade e interoperabilidade [83].

É utilizado para padronizar imagens de todos os tipos, como ressonâncias magnéticas, tomografias computadorizadas, radiografias, mamografias etc., para que sejam armazenadas em formato único, permitindo a troca entre equipamentos de marcas distintas. Ao contrário de outros formatos de arquivo de imagem, como JPEG ou TIFF, os arquivos nesse padrão não são reconhecidos por softwares de leitura de imagens comuns pelos sistemas operacionais. Para visualizar este tipo de arquivo, é necessário usar um visualizador DICOM, que interpreta as informações do arquivo e os exibe como uma imagem [84].

A transferência segura e eficiente de imagens médicas com padrão DICOM, são de extrema importância para o diagnóstico preciso e o tratamento eficaz dos pacientes. Nesta dissertação, exploraremos como a integração da blockchain na transferência de arquivos DICOM pode melhorar a segurança, a privacidade e a interoperabilidade dos dados médicos.

A interoperabilidade fortalece a segurança dos dados, protege a identidade dos pacientes e utiliza criptografia de chave pública e privada, prova de trabalho e um sistema distribuído de consenso de dados para garantir a confiabilidade das informações. É o esquema de criptografia de chave pública e privada responsável por criar camadas de permissão de identidade distintos, garantindo integridade e imutabilidade dos dados.

A implementação na Blockchain na transferência de arquivos DICOM envolve:

1. Digitalização das Imagens Médicas: As imagens são digitalizadas e convertidas para o formato DICOM, garantindo compatibilidade com sistemas de imagens médicas.

2. Armazenamento na Blockchain: As imagens DICOM são carregadas para a blockchain, onde são armazenadas de forma segura e imutável.

3. Gerenciamento de Acesso: Através dos Smart Contracts e criptografia de chave pública e privada e controles de acesso, são implementados na blockchain mecanismo para que apenas as partes autorizadas possam visualizar e compartilhar as imagens médicas.

Embora exista benefícios na transferência de arquivos DICOM, também há questões éticas e regulatórias, especialmente no que diz respeito à privacidade dos pacientes e conformidade com regulamentações de saúde, como o GDPR (Regulamento Geral de Proteção de Dados) na União Europeia e a HIPAA (Lei de Portabilidade e Responsabilidade de Seguro Saúde) nos Estados Unidos. É fundamental que a implementação respeite essas diretrizes e proteja os direitos dos pacientes. Existem desafios a serem superados, mas o potencial dessa

tecnologia promove uma assistência médica mais eficiente e centrada no paciente e serve como um registro distribuído de imagens médicas, facilitando a interoperabilidade entre diferentes sistemas de saúde e instituições médicas [85].

No site, https://nbia.cancerimagingarchive.net/nbia-search/, tem-se uma plataforma online que faz parte do Cancer Imaging Archive (TCIA), visualizado na figura 16, é um repositório de imagens médicas acessível ao público que fornece recursos de pesquisa [86].

Figura 16: Plataforma de imagens médicas em padrão DICOM.

Fonte: Autor, 2024.

A imagem utilizada que será armazenada na Blockchain é fornecida a partir desta plataforma. Na figura 17, visualiza-se imagens no padrão DICOM desse banco de dados.

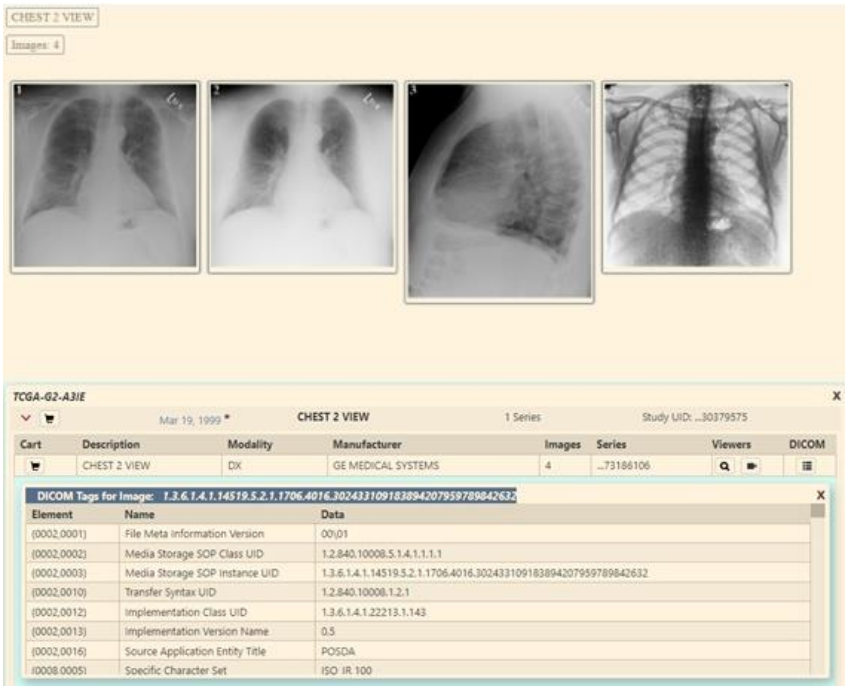

Figura 17: Visualização de Imagem em padrão DICOM.

Fonte: Cancer Imaging Archive, 2024.

5 RESULTADOS E DISCUSSÕES

5.1 Apresentação

Este trabalho foi elaborado como um estudo piloto para o compartilhamento de imagens médicas no formato Digital Imaging and Communications in Medicine (DICOM), com o emprego da blockchain para armazenamento de metadados de arquivos de imagem. Os arquivos de imagens DICOM podem ser transferidos das bases de dados ou oráculos dos provedores de saúde ou de usuários para a Blockchain.

5.2 General Purpose Token (GPToken)

O General Purpose Token (GPToken), um script de token (Smart Contracts), construído com a plataforma de desenvolvimento de contrato inteligente sCrypt-TS foi projetado para funcionar na rede Blockchain do Bitcoin. GPToken é um protocolo de token em UTXO com definição de funcionalidades. Possui a capacidade de incluir dados nas transações, como o envio de dados de saúde de pacientes, tal como a proposta desta dissertação, no caso específico, simularemos envio de imagens médica no formato DICOM. A versão atual do script de token inclui 10 funções está atualmente disponível para testes no TestNet e MainNet da BSV Blockchain por meio da página experimental websvmenu, como vê-se na figura 18 [82].

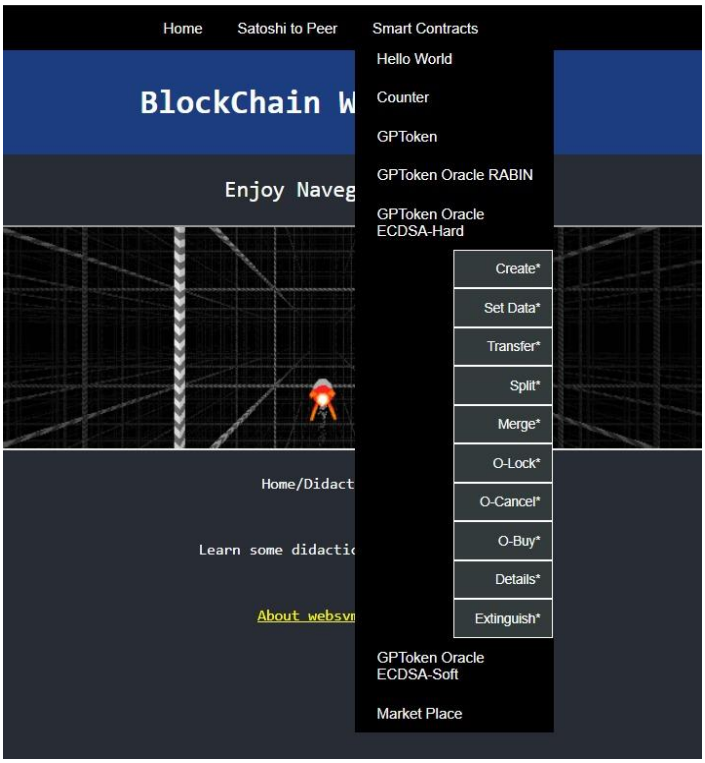

Figura 18: Página experimental e menu das funções do GPToken.
Fonte: Autor, 2024.

A interface permite que os usuários interajam com o Smart Contracts, a página da web, o GPToken. Para iniciar os procedimentos de armazenamento de arquivos e envio à blockchain, é necessário acessar (HOME/ACCESS) no GPToken, e inserir a chave privada em formato hexadecimal, como demonstrado na figura 19.

Figura 19: Acesso ao GPToken.

Fonte: Autor, 2024.

Após a inserção da chave privada ou senha, o usuário pode alternar entre as redes TestNet e MainNet, e o formato do endereço mudará imediatamente, mas o formato da SEC Pub Key permanecerá o mesmo. O usuário também pode alterar o formato de compactação da chave pública e o endereço mudará para cada tipo de formato de compactação [81].

A principal aplicação a ser utilizada no GPToken para envio de informações médicas à rede será simulada usando a funcionalidade SET DATA, destinado a inserir dados no token. Antes de realizar o envio, é necessário criar o token com uma determinada quantidade de satoshis (sat) atrelados a ele, e o número específico de unidades definido pelo emissor através da funcionalidade CREATE.

Demonstrado na figura 20, observa-se a criação do token com 1 unidades e lastreado com 1 sat. O estado atual deste token está na transação identificada como Transaction Identication (TXID) observado em tela.

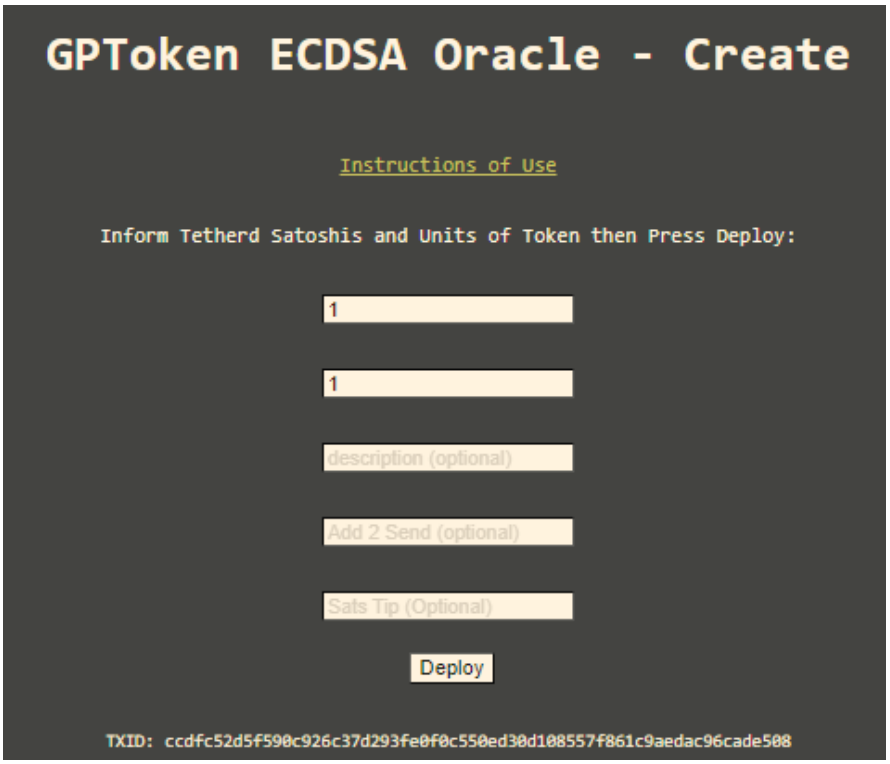

Figura 20: Create.

Fonte: Autor, 2024.

O TXID representa um identificador exclusivo atribuído a cada transação na blockchain. A cada execução de uma transação na blockchain, é gerado um TXID específico. Esse identificador possibilita o rastreamento e a verificação detalhada das transações por meio de exploradores de blockchain, como o WhatsOnchain, que fornece acesso a blocos BSV, transações, atividade de endereços, dados On Chain, estatísticas e muito mais. Ou seja, ao utilizar o TXID, o identificador exclusivo da transação, em qualquer serviço de recuperação disponível na rede, é possível acessar informações específicas sobre a transação.

Abaixo, o TXID obtido na funcionalidade CREATE:

TXID: ccdfc52d5f590c926c37d293fe0f0c550ed30d108557f861c9aedac96cade508

Pode-se inserir um dado, um texto ou arquivo em qualquer padrão nesse token criado. Para isso, utiliza-se a funcionalidade SET DATA com o último estado através do TXID no CREAT. Na figura 20, demonstra-se a inserção do dado no token, do arquivo em formato

DICOM de uma tomografia computadorizada de abdômen e na figura 21, a mesma imagem, mas em formato JPEG, meramente como visualização da imagem em formato DICOM.

Figura 21: Set data.

Fonte: Autor, 2024.

O dado foi incluído no token e esse mudou de estado, pois agora tem um dado incluído. O TXID do último estado obtido, após inserir o dado é:

TXID: f9db1d57cf8fc61f595b09c052f3d1abdf7fadb9851c5d2992e2ed002c210b67

A imagem armazenada na blockchain no padrão DICOM, é vista na figura 22 em formato JPEG, e posteriormente será demonstrada no visualizador DICOM online.

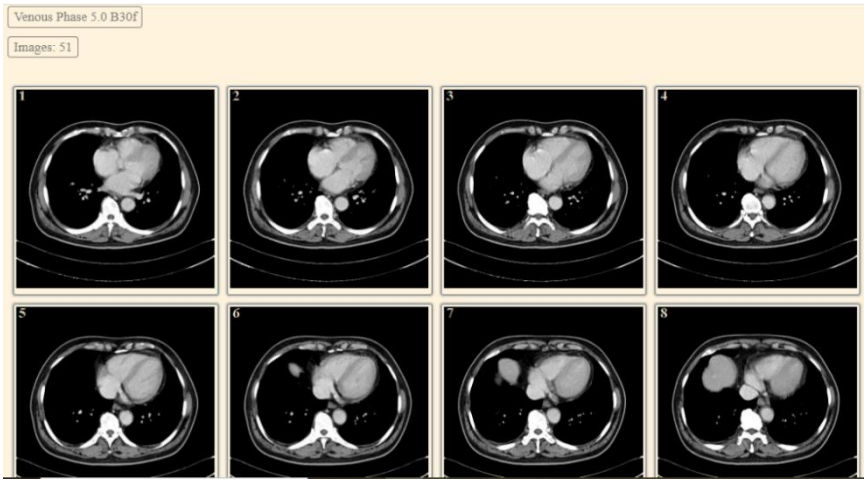

Figura 22: Imagem JPEG de tomografia computadorizada.

Fonte: Autor, 2024.

Com o TXID do último estado pode se recuperar a imagem obtida através da funcionalidade READ FROM TRANSACTION e verificar a transação armazenada na Blockchain por meio da WhatsOnchain. A visualização da tomografia inserida não pode ser visualizada no GPToken na funcionalidade READ, somente com os visualizadores DICOM.

Como citado anteriormente, softwares de leitura de imagens comuns pelos sistemas operacionais tradicionais não visualizam arquivos DICOM, sendo necessário usar um visualizador DICOM, que os exiba como imagem, podendo ser visualizadores DICOM online ou leitores DICOM desktop em computadores locais. Será utilizado para visualização da imagem DICOM o IMAIOS DICOM Viewer, um visualizador online.

Primeiramente, demonstrar-se-á a recuperação da imagem por meio do READ, como na figura 23, utilizando o último TXID. Sendo também possível baixar o arquivo para um computador, mas não sendo possível visualizá-lo, tanto no GPToken como em leitores comuns.

Figura 23: Read from transaction.

Fonte: Autor, 2024.

Realizado o download a partir do GPToken, o arquivo baixado em formato DICOM foi importado para o software IMAIOS, o visualizador online, e na figura 24, tem-se a visualização em padrão DICOM dessa imagem, já armazenada na blockchain anteriormente através do Set Data e lida através do Read from Transaction.

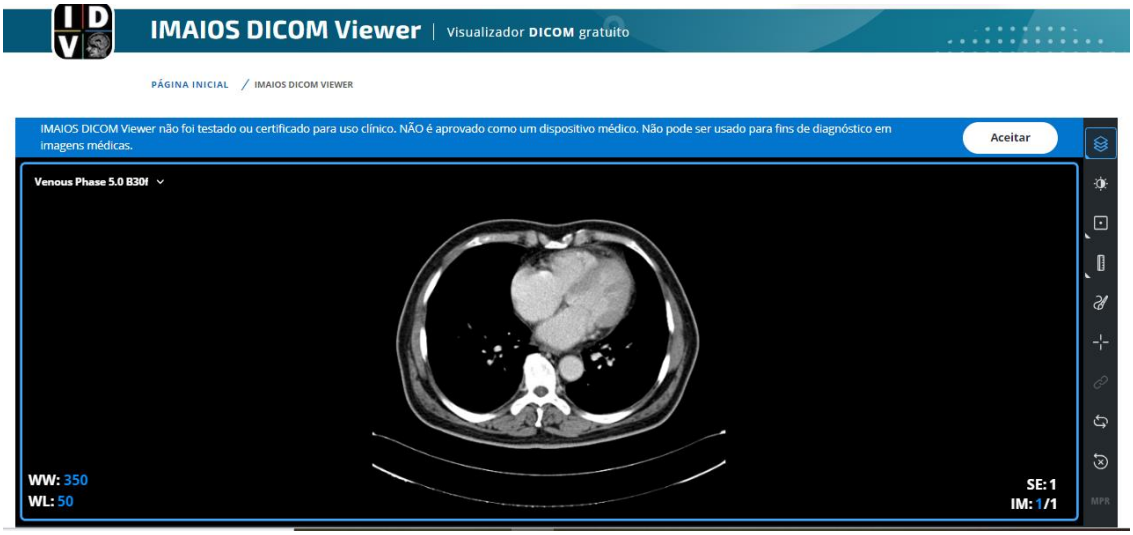

Figura 24: Visualizador online IMAIO.

Fonte: Autor, 2024.

Após a leitura, através da funcionalidade READ FROM TRANSACTION e com o download da imagem, e posterior visualização pelo IMAIOS no formato DICOM, segue-se através do WhatsOnChain para constatar a transação incluída na rede Blockchain, conforme figura 25. Utiliza-se o último TXID obtido em Set Data para fazer a pesquisa no WhatsOnChain.

Figura 25: Informação recuperada da transação na WhatsOnChain.

Fonte: Autor, 2024.

De acordo com a figura 25, observa-se o ID da transação, o número do bloco no qual a transação foi incluída, carimbo de data/hora em que o bloco foi criado pelos validadores da transação (Timestamp), a versão do bloco, além da taxa de transação e velocidade da transação.

A blockchain BSV oferece não apenas recursos de escalabilidade, mas também a capacidade de incluir tipos arbitrários de dados dentro de transações, tal como incluímos uma imagem de tomografia. Isso significa que qualquer tipo de dado pode ser inserido em uma transação e posteriormente recuperado usando o ID único da transação por meio de qualquer serviço de recuperação, tal como o WhatsOnChain.

Recordando que o cabeçalho do bloco inclui informações como a versão do protocolo, o timestamp, o hash do bloco anterior, uma Prova de Trabalho, a versão do bloco, um nonce (um número aleatório usado na mineração), a raiz da árvore de Merkle, que é um resumo criptográfico de todas as transações incluídas no bloco. Observa-se a capacidade do Bitcoin SV de adicionar blocos stamps às transações para incluir metadados adicionais que podem ser anexados a uma transação na blockchain. São esses blocos stamps permitem que os usuários insiram e recuperem dados arbitrários de imagem na blockchain [57].

Observa-se na figura 26, as saídas da transação, uma das quais inclui os dados do nosso contrato criado e na entrada tem-se o endereço da carteira do remetente.

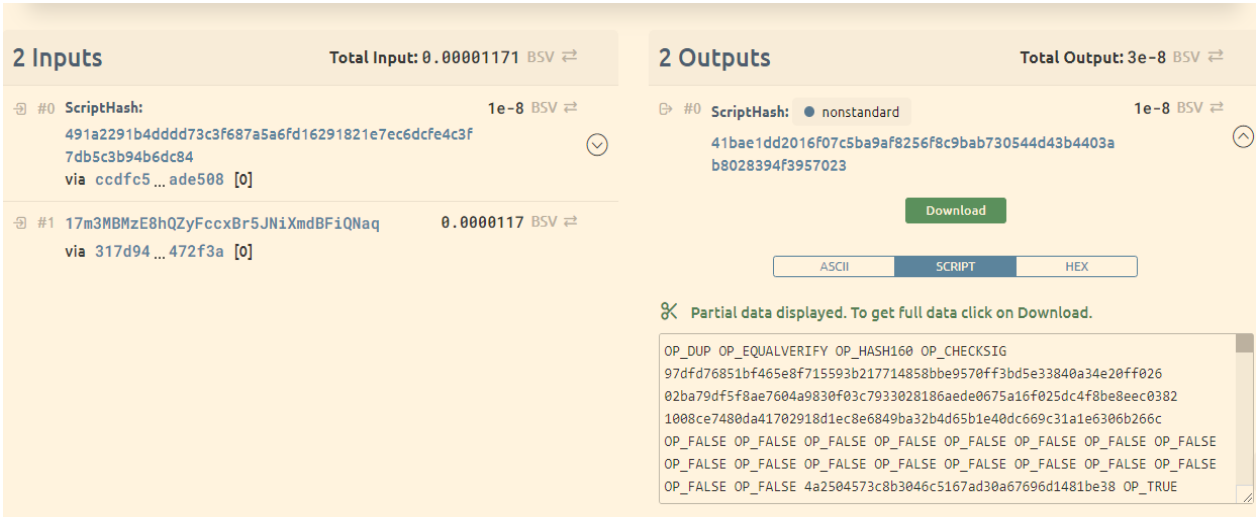

Figura 26: Informação recuperada da transação na WhatsOnChain

Fonte: Autor, 2024.

5.3 Aplicabilidade Médica

No decorrer deste trabalho, teve-se a oportunidade de explorar diversas fontes de dados para embasar as análises. Utilizar diversas fontes de imagens médicas seria de grande enriquecimento. No entanto, devido à ausência de autorização do Conselho de Ética para o uso de tais imagens, optou-se por alternativas para viabilização dos resultados.

Foram encontrados desafios ao tentar obter autorização ao Conselho de Ética para a utilização de imagens médicas devido às complexidades. O processo de solicitação envolve uma série de etapas e procedimentos, desde a preparação da documentação necessária até a submissão formal da solicitação. Após a solicitação, o processo de avaliação pode consumir um considerável tempo. Ainda podem ser solicitadas informações adicionais sobre a pesquisa proposta, prolongando ainda mais o processo.

Considerando as dificuldades na solicitação ao Conselho de Ética, optou-se por não incluir imagens médicas que necessitassem autorização. Tentativas de contornar essa falta incluíram buscar alternativas, como bancos de dados abertos, porém, encontraram-se limitações. Embora esses recursos oferecessem vantagens em acessibilidade e disponibilidade, a escassez de informações limitou a extensão e profundidade da pesquisa, afetando a variedade dos resultados na dissertação.

Tipos de imagens médicas, como ressonância magnética, tomografia computadorizada, ultrassonografia, radiografia, angiografia, PET-CT (Tomografia por Emissão de Pósitrons) e ultrassom Doppler, são usados para demonstrar uma variedade de condições e doenças em contextos médicos. Essas imagens são essenciais para o diagnóstico, monitoramento e tratamento de pacientes, oferecendo uma variedade de dados.

Dentro desse contexto, para tornar interoperável um sistema médico, pode-se explorar outras formas de coleta de dados e integração de informações. Uma abordagem eficaz seria implementar protocolos de interoperabilidade, como o DICOM, para integrar como fonte de dados a um sistema médico. Essa integração permite a análise preditiva, desde que sejam estritamente respeitadas as políticas de privacidade e segurança dos dados, ampliando o acesso a uma variedade de imagens médicas, enriquecendo as análises e diagnósticos clínicos. Dessa forma, automatizar processos de triagem e identificação de padrões em imagens médicas, contribui para uma análise mais eficiente e precisa.

6 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho implementou um Sistema de Acesso e Compartilhamento de imagens médicas no formato Digital Imaging and Communications in Medicine (DICOM), utilizando a blockchain do Bitcoin para armazenamento de arquivos de imagem.

Para a etapa de desenvolvimento do protocolo da camada de aplicação Back-end do Smart Contracts foi realizado a especificação das funcionalidades do Smart Contracts. Para a camada Front-end Web, foi projetado a interface do usuário com definição dos elementos visuais e a integração da interface com o Smart Contracts na camada de aplicação back-end.

A integração das camadas resultou no GPToken, possibilitada pela plataforma de desenvolvimento de contratos inteligentes sCrypt-TS. O Smart Contracts construído com a plataforma sCrypt-TS foi testado para simular envio de imagens médica no formato DICOM para a rede blockchain e posteriormente possibilitada a recuperação pelo usuário.

Para trabalhos futuros, recomenda-se a construção de um conversor de imagens para formatos DICOM e outros formatos de imagens médicas integrado à aplicação em blockchain. Isso porque a solução implementada através do GPToken não permite a visualização direta do dado de imagem. A integração do protótipo com suporte ao formato DICOM, formato utilizado como exemplo, mas com suporte a outros formatos, permitiria maior compatibilidade com sistemas médicos e facilitaria o uso em ambientes clínicos. Além disso, a inclusão dessa funcionalidade aumentaria a utilidade e a adoção da aplicação em cenários médicos.

A integração da blockchain na transferência de arquivos DICOM representa um avanço significativo na digitalização de dados médicos, uma inovação com aplicação na BSV demonstrada nesta dissertação. Isso é importante porque a maioria das aplicações com contratos inteligentes voltados para soluções médicas normalmente fazem uso de outras blockchains.

Ao utilizar a blockchain do Bitcoin para transferir arquivos DICOM e digitalizar dados médicos, é possível aproveitar os recursos específicos dessa blockchain, como sua capacidade de escalabilidade e a habilidade de incluir tipos arbitrários de dados em transações. Isso pode levar a uma maior eficiência, e integridade dos dados médicos, além de simplificar os processos de compartilhamento e acesso aos registros médicos através da utilização dos Smart Contracts.

7 REFERÊNCIAS BIBLIOGRÁFICAS

[1] L. Vítor, "Saúde Digital: a Interoperabilidade e a Tecnologia Blockchain", Dissertação de Mestrado, Universidade da Beira Interior, Covilhã, 2020.[Online]. Disponível em: https://ubibliorum.ubi.pt/bitstream/10400.6/10600/1/7333_15808.pdf

[2] M. Ashraf *et al.*, "Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture". IEEE 2018, 6, 32700 - 32726.

[3] K.N. Griggs *et al.*, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring". J. Med. Syst. 2018, 2.

[4] T. Pinheiro, J. Oliveira, J. Guedes, M. Oliveira, J. Neves, C. Cruz. Acesso e Compartilhamento de Dados de Saúde em Blockchain Usando Smart Contracts. In: XVI Simpósio Brasileiro de Automação Inteligente (SBAI 2023), 2023, Manaus.

[5] J. Neves, J. Oliveira, M. Oliveira, C. Cruz, T. Pinheiro. Comparative Analysis between a Private Network Micro-Blockchain IoT and an open Blockchain in the Data Collection of Decentralized Agents In: XVI Simpósio Brasileiro de Automação Inteligente (SBAI2023), 2023, Manaus.

[6] J. Oliveira , J. Guedes, M. Oliveira , J. Neves, C. Cruz, T. Pinheiro. IoT and Automation via Blockchain – A Simple Solution In: XVI Simpósio Brasileiro de Automação Inteligente (SBAI 2023), 2023, Manaus.

[7] J. Morsch, "Blockchain na saúde: o que é, para que serve e exemplos de uso," Telemedicinamorsch, Disponível: https://telemedicinamorsch.com.br/blog/blockchain-na-saude. Acesso: Jun. 09, 2023.

[8] WikiBitcoin, "Welcome to the Bitcoin Wiki," Associação Bitcoin, Disponível: https://wiki.bitcoinsv.io/index.php/Main_Page. Accessed: Sept. 28, 2023.

[9] "O que é blockchain? Conheça a tecnologia que torna as transações com criptos possíveis," Infomoney, Disponível: https://www.infomoney.com.br/guias/blockchain/. Accessed: Sept. 26, 2023.

[10] RJ. Krawiec *et al*., "Blockchain: Opportunities for healthcare," Deloitte, New York, Aug. 2016.

[11] "Blockchain: Technology in life Sciences and Health," BioRegio STERN, Stuttgart, Dec. 2022.

[12] R.Joshi,"Blockchain in Healthcare & Life Sciences," PreScouter, Available: https://www.prescouter.com/press/blockchain-in-healthcare-life-sciences/. Accessed:Sept.07, 2023.

[13] "The Challenge of Health Care Fraud," NHCAA Institute, Available: https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud. Accessed: Oct. 16, 2023.

[14] A.v. Dijk, R.Theunissen, "Deloitte Tech Trends 2023," Deloitte, Available: https://www2.deloitte.com/nl/nl/pages/enterprise-technology-and-performance/articles/technology-trends.html. Accessed: Sept. 12, 2023.

[15] T.Smith, " Blockchain to blockchains in life sciences and health care," Deloitte, New York, 2023.

[16]D.Kuhn,"Bitcoin–Daily Number of Transactions," CoinDesk, Available: httpswww.coindesk.comconsensus-magazine20230501bitcoin-set-new-record-of-daily-transactions-the-same-day-the-us-government-quietly-engineered-a-bank-buyout.Accessed: Oct. 27, 2023.

[17] G. Lucas, "BSV blockchain sets new world record with 128M transactions in 24 hours," CoinDesk, Available: https://coingeek.com/bsv-blockchain-sets-a-new-world-record-with-128m-transactions-in-24-hours/. Accessed: Oct. 27, 2023.

[18] J. Baillieu , "Exploring and deploying blockchain solutions in the life sciences and healthcare sectors,"European Pharmaceutical Review, Available: https://www.europeanpharmaceuticalreview.com/article/126761/exploring-and-deploying blockchain-solutions-in-the-life-sciences-andhealthcare-sectors/. Accessed: Aug. 24, 2023.

[19] Hasselgren et al., "GDPR Compliance for Blockchain Applications in Healthcare," Available: https://arxiv.org/pdf/2009.12913.pdf. Accessed: Aug. 24, 2023.

[20] E. Politou *et al*., "Blockchain Mutability: Challenges and Proposed Solutions," IEEE Transactions on Emerging Topics in Computing, 9, 1972 - 1986. Dec. 2021

[21] J. Holden, "Prescrypt Brings Medical Prescriptions to the Blockchain," Bitcoin.com, Available: https://news.bitcoin.com/prescrypt-blockchain-prescriptions/. Accessed: Sept. 22, 2023.

[22] L. Engelen, "Blockchain for healthcare and your banking card," Linkedin, Available: https://www.linkedin.com/pulse/blockchain-healthcare-your-banking-card-lucien-engelen/. Accessed: Sept. 29, 2023.

[23] A. Azarias *et al.*, " MedRec prototype for electronic health records and medical research data," Available:https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf. Accessed: Jul. 03, 2023.

[24] "Change Healthcare Introduces Enterprise Blockchain for Healthcare," BusinessWire, Available: https://www.businesswire.com/news/home/20170925005820/en/Change-Healthcare-Introduces-Enterprise-Blockchain-for-Healthcare. Accessed: Jul. 27, 2023.

[25] G. Prisco, "Blockchain for healthcare: Gem launches Gem Health Network with Philips Blockchain Lab," Bitcoin Magazine, Available: https://bitcoinmagazine.com/business/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938. Accessed: Jul. 27, 2023.

[26] W.Suberg, "Factom announces partnership with HealthNautica," Cointelegraph, Available: https://cointelegraph.com/news/french-senate-bitcoin-offers-multiple-opportunities-for-the-future. Accessed: Jul. 29, 2023.

[27] J. Roberts, "Big Pharma Turns to Blockchain to Track Meds," Fortune, Available: http://fortune.com/2017/09/21/ pharma-blockchain/. Accessed: Jul. 29, 2023.

[28] A. Dearment, "United States : Boehringer Ingelheim (Canada) Ltd. and IBM Canada Announce Firt of its Kind Collaboration to Integrate Blockchain Technology into Clinical Trials," MedCityNews, Available: https://medcitynews.com/2019/02/boehringer-ingelheim-ibm-to-study-blockchain-in-clinical-trials/. Accessed: Jul. 29, 2023.

[29] "Discover the top 10 trends and innovations in the pharmaceutical industry in 2022,"

StartUs, Available: https://www.startusinsights.com/innovators-guide/top-10-pharma-industry-trends-innovations-in-2021/#blockchain. Accessed: Jul. 20, 2023.

[30] "The first comprehensive blockchain-supported personal care record platform has been launched," Healthcare Digital Magazine, Available: https://healthcare-digital.com/digital-healthcare/first-comprehensive-blockchain-supported personal-care-record-platform-has-been-launched. Accessed: Aug. 14, 2023.

[31] "Towards the future of healthcare with interoperability," Deloitte, Available: https://www2.deloitte.com/de/de/pages/life-sciences-and-healthcare/articles/interoperabilitaet-im-gesundheitswesen.html.Accessed: Aug. 14, 2023.

[32] A. Azarias *et al.*, " MedRec prototype for electronic health records and medical research data," Available: https://www.healthit.gov/sites/default/files/5-56

[33] A. Dubovitskaya *et al.*, "Secure and Trustable Electronic Medical Records Sharing using Blockchain," ResearchGate, Aug 24, 2017. [Online], Available: https://www.researchgate.net/publication/319928609_Secure_and_Trustable_Electronic_Medical_Records_Sharing_using_Blockchain. [Accessed: Jul. 18, 2023].

[34] O. Ossipova *et al.,* (2023, Aug.) "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," Journal of Medical Systems. [Online]. 42,130(2018). Available: https://link.springer.com/article/10.1007/s10916-018-0982-x#additional-information

[35] P. Vieira, “Secure storage and sharing of health data in a Blockchain environment”, M.S. thesis, Faculty of Sciences and Technology, NOVA University Lisbon, Lisbon, 2018.

[36] S. Chakraborty et al., “A Secure Healthcare System Design Framework using Blockchain Technology,” 2019 21st International Conference on Advanced Communication Technology (ICACT), DOI: 10.23919/ICACT.2019.8701983.

[37] N. Rodrigues, “Concessão de Permissão a Dados de Saúde Baseada em Blockchain,” Sociedade Brasileira de Computação, 263 - 274. Mar. 2019

[38] P. H. Luan and T.H.Tran, “A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract,” 2018 IEEE Globecom Workshops (GC Wkshps), DOI: 10.1109/GLOCOMW.2018.8644164.

[39] O. Ukanah and C. Obimbo, “Blockchain Application in Healthcare,” 2021 International Conference on Technological Advancements and Innovations (ICTAI), DOI: 10.1109/ICTAI53825.2021.9673187.

[40] F. Jamil *et al.,* (2023, Sept.) “Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals ,” Journal of Medical Systems. [Online]. 2020, 20(8), 2195. Available: https://www.mdpi.com/1424-8220/20/8/2195

[41] F. Jamil *et al.,* (2023, Sept.) “A Patient-Centric Health Information Exchange Framework Using Blockchain Technology,” Journal of BioMedical and Health Informatics. [Online]. 2020, 24(8), 2195. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9090282

[42] S. Dass *et al.*, “A Blockchain based Electronic Medical Health Records Framework using Smart Contracts,” 2021 International Conference on Computer Communication and Informatics (ICCCI), DOI: 10.1109/ICCCI50826.2021.9402689.

[43] A. Maghraby *et al.*, “Applied Blockchain Technology in Saudi Arabia Electronic Health Records,” 2021 International Conference on Computational Science and Computational Intelligence (CSCI), DOI: 10.1109/CSCI54926.2021.00070.

[44] A. Venkata *et al.*, “Decentralized Secure Personal Health Record Monitoring System using Blockchain,” 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), DOI: 10.1109/i-PACT52855.2021.9696931.

[45] H. Wang and R. Zhou, “The Application of Blockchain to Electronic Health Record Systems: A Review,” 2021 International Conference on Information Technology and Biomedical Engineering (ICITBE), DOI: 10.1109/ICITBE54178.2021.00092.

[46] K. Ramar *et al.*, “Digital Healthcare using Blockchain,” 2022 1st International Conference on Computational Science and Technology (ICCST), DOI: 10.1109/ICCST55948.2022.10040411.

[47] M. Mittal *et al.,* “An Electronic Health Record Management System Based on Blockchain Technology,” 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP), DOI: 10.1109/ICFIRTP56122.2022.10059456.

[48] S. Singh *et al.*, “MedEHR-Eletronic Health record using blockchain,” 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), DOI: 10.1109/CICTN57981.2023.10141053.

[49] A. Galaba *et al.*, “Significance of Blockchain Technology in the Healthcare Sector,” 2023 International Conference on Inventive Computation Technologies (ICICT), DOI: 10.1109/ICICT57646.2023.10134196.

[50] A. Vernekar *et al.,* “Sharding-based scalability enhancement of blockchain-based health application,” 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT), DOI: 10.1109/ICCPCT58313.2023.10245363.

[51] M. Mittal *et al.,* "An Electronic Health Record Management System Based on Blockchain Technology," 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP), DOI: 10.1109/ICFIRTP56122.2022.10059456.

[52] H. Agrawal *et al.,* "Digital Health Data Supervision using Blockchain in Ethereum Testnet," 2023 2st International Conference on Augmented Intelligence and Sustainable Systems (ICAISS 2023), DOI: 10.1109/ICAISS58487.2023.10250620.

[53] J. Godwin *et al.,* "Electronic Healthcare Management System using Blockchain Technology," 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT), DOI: 10.1109/ICCPCT58313.2023.10245668.

[54] N. Rodrigues, "Concessão de Permissão a Dados de Saúde Baseada em Blockchain", Dissertação de mestrado, Universidade Federal de Goiás, Goiás, 2020.

[55] R. Chan, "Blockchain data structure," Linkedin, Available: https://www.linkedin.com/pulse/blockchain-data-structure-ronald-chan. Accessed: Apr. 22, 2023.

[56] A. Fialho, "Opcodes used in Bitcoin Script ," The Capital Advisor, Available:https://wiki.bitcoinsv.io/index.php/Opcodes_used_in_Bitcoin_Script. Accessed: June. 09, 2023.

[57] "Bitcoin Primitives: Digital Signatures," BSV Association, Available: https://academy.bsvblockchain.org/course/bitcoin-primitives-digital-signatures. Accessed: Sept. 22, 2023.

[58] "Target," Bitcoin Wiki, Available: https://en.bitcoin.it/wiki/Target. Accessed: Sept. 22, 2023.

[59] "Ripemd-160," Bitcoin Association, Available: https://wiki.bitcoinsv.io/index.php/RIPEMD-160. Accessed: Sept. 22, 2023.

[60] "DER," Stack Exchange, Available: https://bitcoin.stackexchange.com/questions/92680/what-are-the-der-signature-and-sec-format. Accessed: Sept. 22, 2023.

[61] "Blockchain," Departamento de Engenharia Eletrônica da Universidade Federal do Rio de Janeiro, Available: https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-vf/blockchain/security.html. Accessed: Sept. 22, 2023.

[62] "Proof of work," Bitcoin Wiki, Available: https://en.bitcoin.it/wiki/Proof_of_work. Accessed: Sept. 22, 2023.

[63] A. Back, "Hashcash - A Denial of Service Counter- Measure," Satoshi Nakamoto Institute, Aug 01, 2002. [Online], Available: http://www.thewest.com.au. Accessed: Sept. 18, 2023.

[64] "The Bitcoin Network," Bitcoin Association, Available: https://wiki.bitcoinsv.io/index.php/The_Bitcoin_Network.Accessed: Sept. 22, 2023.

[65] "BSV Blockchain History," BSV Blockchain, Available: https://www.bsvblockchain.org/history. Accessed: Sept. 22, 2023.

[66] G. Lucas, "BSV blockchain sets new world record with 128M transactions in 24 hours," Coingeek, Available: https://coingeek.com/bsv-blockchain-sets-a-new-world-record-with-128m-transactions-in-24-hours/. Accessed: Sept. 22, 2023.

[67] J. Southurst, "BSV Blockchain Association explains recent network congestion," Coingeek, Available: https://coingeek.com/bsv-blockchain-association-explains-recent-network-congestion. Accessed: Sept. 22, 2023.

[68] "Block Wiever," Teranode, Available: https://teranode.bsvblockchain.org/viewer/?s=08. Accessed: Mar. 11, 2024.

[69] V. Buterin, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum, Nov 24, 2013. [Online], Available: https://ethereum.org/en/whitepaper/. Accessed: Sept. 18, 2023.

[70] Crisgarner, “Ethereum: A Secure Decentralized Generalized Transaction Ledger,” Medium, Available:https://medium.com/ethereum-foundation-devcon-scholars/ethereum-a-secure-decentralised-generalised-transaction-ledger-7a402984dacb. Accessed: Sept. 22, 2023.

[71] R. Linus, “BitVM: Compute Anything on Bitcoin,” Ethereum, Oct 09, 2023. [Online], Available: https://bitvm.org/bitvm.pdf. Accessed: Oct. 12, 2023.

[72]Y.Majuri, “Smart Contracts #1: Introduction,” Medium, Available:https://yakkomajuri.medium.com/smart-contracts-1-introdu%C3%A7%C3%A3o-c91d38c44aaf. Accessed: Oct. 12, 2023.

[73] S. Bruno, “Smart Contracts: conceitos, limitações, aplicabilidade e desafios,”Available: https://www.cidp.pt/revistas/rjlb/2018/6/2018_06_2771_2808.pdf. Accessed: Oct. 05, 2023

[74] D. Pokharna, “Develop DApps on Ethereum,” Medium, Available: https://medium.com/technologymadeeasy/develop-dapps-on-ethereum-tutorial-series-for-beginners-part-1-basic-terminology-866d2ce4cf34. Accessed: Oct. 05, 2023.

[75] E. Isabella, “Smart Contract Development: A Step-by-Step Guide,” Medium, Available: https://blog.cryptostars.is/smart-contract-development-a-step-by-step-guide-e0c419941b90. Accessed: Oct. 11, 2023.

[76] sCrypt, “The First High-Level Language Smart Contract on BTC,” Medium, Available: https://xiaohuiliu.medium.com/the-first-high-level-language-smart-contract-on-btc-6db9a4b788d4. Accessed: Mar. 07, 2024.

[77] “Opcodes used in Bitcoin Sacript,” Bitcoin Association, Available: https://wiki.bitcoinsv.io/index.php/Opcodes_used_in_Bitcoin_Script. Accessed: Mar. 07, 2024.

[78]“Pay to Public Key Hash (P2PKH),”Bitcoin Association,Available: https://wiki.bitcoinsv.io/index.php/Bitcoin_Transactions#Pay_to_Public_Key_Hash_.28P2PKH.29

[79] “Building on Bitcoin,” Bitcoin Association, Available: https://wiki.bitcoinsv.io/index.php/Building_on_Bitcoin. Accessed: Sept. 26, 2023.

[80] “Application layer protocol,” Bitcoin Association, Available: https://wiki.bitcoinsv.io/index.php/Application_layer_protocol. Accessed: Sept. 27, 2023. 7

[81] C. Cruz, “UTXO vs Blockchains baseados em contas,” https://medium.com/@cktcracker/utxo-vs-account-based-blockchains-bb648cbf4502. Accessed: Nov. 7, 2023.

[82] C. Cruz, “General Purpose Token GPToken,” Medium, Available: https://medium.com/@cktcracker/general-purpose-token-gptoken-6e4a06c3f01e. Accessed: Nov. 7, 2023.

[83] “Formato DICOM,” Maislaudo, Available:https://maislaudo.com.br/blog/entenda-o-que-e-o-formato-dicom-e-conheca-os-seus-beneficios/. Accessed: Fev. 7, 2024.

[84] “DICOM e PACS,” medcloud, Available: https://blog.medcloud.com.br/dicom-e-pacs-o-que-sao-e-quais-as-diferencas/. Accessed: Fev. 7, 2024.

[85] Imaios DICOM Viewer, Available:https://www.imaios.com/br/imaios-dicom-viewer.Accessed: Fev. 7, 2024.

[86] Cancer Imaging Archive, Available: https://nbia.cancerimagingarchive.net/nbia-search/. Accessed: Fev. 7, 2024.