Este trabalho foi originalmente submetido em Agosto de 2021, na 23ª Jornada de Iniciação Científica na Universidade Católica de Pernambuco (UNICAP). Inicialmente entregue como o relatório final para o PIBIC 2020-2021, este trabalho foi orientado pelo professor Sérgio Murilo Maciel Fernandes. Esta versão foi resumida para conter apenas o conteúdo da pesquisa, descartando os demais itens presentes no relatório final de atividades.

Investigação da utilização de Contratos Inteligentes, baseados no paradigma Blockchain, em áreas da saúde, especialmente, fisioterapia e reabilitação

3.1 INTRODUÇÃO

Com o passar dos anos, as atividades manuais desenvolvidas e desempenhadas por seres-humanos vem sendo digitalizadas e automatizadas por computadores. Esse processo de transformação e adaptação digital diminui a dependência da confiabilidade humana, reduz custos e minimiza impactos de fenômenos incontroláveis da natureza. Como reflexo desse desenvolvimento tecnológico, atividades diárias, como vendas, passam também a acontecer digitalmente pela internet.

Apesar das facilidades e vantagens que o meio virtual pode proporcionar, o processo não é repensado para acontecer digitalmente; é apenas um espelho do passo-a-passo que ocorreria no presencial. Segundo Nakamoto [1], as transações online são parte de um sistema altamente baseado na confiança de que mediadores externos sirvam como segurança para os participantes.

Levando em consideração as fraquezas do sistema atual [1], foi desenvolvida então uma alternativa: as criptomoedas. Surgindo em 2008 com o advento do Bitcoin [2], elas são a promessa de "um sistema de pagamento eletrônico baseado em prova criptográfica ao invés de confiança, permitindo que qualquer um realize transações diretamente com a outra parte, sem necessidade de um agente terceiro" [1].

Nesse cenário, o *blockchain* é o conceito responsável por garantir o funcionamento do sistema, agindo como o *ledger* [3] (livro-razão) das transações e garantindo a confiabilidade através de fatores como: função criptográfica *hash*, assinaturas digitais e algoritmos de consenso [4], sem a necessidade de uma autoridade central de regulação [5] a qual as transações devem ser reportadas e validadas. Esse sistema configura o que é chamado de *trustless network*, onde ambas as partes podem operar sem a necessidade de haver confiança entre si [6].

Bell et. al. [7] afirma que apesar do foco em serviços financeiros, existem diversas outras áreas nas quais o *blockchain* pode ser aplicado de forma disruptiva, sendo algumas delas: eleições, gestão de cadeia de suprimentos, *healthcare* e *smart contracts*. Nick Szabo [8] introduziu o conceito de contratos inteligentes como "um protocolo de transação computadorizado que executa os termos de um contrato". Ele também define como exemplo canônico uma *vending machine* [8]: caso o usuário possua dinheiro suficiente, ele insere o dinheiro na máquina, escolhe um produto, e recebe o troco, encerrando o contrato. Existe também a possibilidade de punir uma das partes [9] caso as cláusulas sejam interrompidas ou não devidamente cumpridas.

Tendo em vista as inovações disruptivas apresentadas previamente, esta pesquisa tem como objetivo investigar como os contratos inteligentes, através do paradigma do *blockchain*, podem ser aplicados na área de *healthcare*, com foco específico em fisioterapia e reabilitação.

3.1.1 Blockchain

Criado por Satoshi Nakamoto para ser a base do Bitcoin, *blockchain* é um registro de informações aberto formado por uma cadeia de blocos de dados, interligados através de um código gerado por uma função *hash*. Por ser aberto, é possível que todos os participantes da rede tenham acesso de leitura aos dados contidos nos blocos. Suas principais características são: descentralização, persistência, anonimato e auditabilidade.

O conceito foi desenvolvido a partir da seguinte problemática: alta dependência em agentes externos para realizar transferências monetárias. Para o seu desenvolvimento, foram levados em consideração fatores como [1]: transações validadas por instituições financeiras não são completamente reversíveis, sendo suscetíveis a fraudes (problemas como *double spending*, por exemplo, que é um cenário onde gasta-se os mesmos fundos duas vezes), existência de taxas adicionais altas, lentidão no processo, entre outros.

Um bloco é um registro criado no momento que uma transação é validada, e é construído a partir dos seguintes parâmetros [10, 11]:

- *Version*: Versão do sistema utilizado;
- *Nonce*: número aleatório, que serve de apoio para cadeias que utilizam o sistema *Proof of Work*;
- *Timestamp*: momento que representa a data e hora de criação do bloco;
- *Previous Block Hash/Digest*: código gerado por uma função *hash* que referencia o bloco anterior a este;
- *Bits*: tamanho do bloco;

• Merkle *Root hash*: código *hash* que referencia a raíz de uma árvore de Merkle, responsável por conter outras *hashes* de outras transações [11].

Para adicionar blocos à cadeia, o *blockchain* utiliza-se dos chamados algoritmos de consenso. Existem diversos, sendo as variações mais conhecidas:

• *Proof of Work* (prova de trabalho): participantes da rede, chamados de "mineradores", são responsáveis por resolver um problema matemático [12] até que o valor da equação seja igual ao valor do *nonce* do bloco.

• *Proof of Stake* (prova de participação): o bloco deve comprovar que possui a quantidade de moedas que deseja gastar. Nesse consenso, comprovar a posse da quantia necessária significa enviar o valor para si mesmo. Os participantes são escolhidos por fatores diferentes da mineração, no entanto, o método de escolha costuma variar dependendo da criptomoeda.

Independente do algoritmo de consenso utilizado, só é possível um *hacker* fraudar uma transação caso ele consiga ter acesso a 51% da rede completa. Em ambos os casos, o custo da compra de poder computacional para realizar tal feito em *blockchains* já estabelecidos é altíssimo, compensando mais o atacante participar justamente. Em casos de *blockchains* que ainda estão em estado inicial, o valor da criptomoeda é insignificante, novamente configurando prejuízo para o atacante.

Existem situações onde dois participantes podem gerar um bloco referente à mesma transação ao mesmo tempo. Nesse caso, ocorre um *fork*, que são dois caminhos paralelos simultâneos. Os desvios seguem normalmente até que um fique maior do que o outro; este então é o que será adicionado à rede, e os blocos do caminho descartado são enviados para a lista de espera, cuja denominação oficial depende da criptomoeda.

Zheng *et al*. [3] afirmam que existem mais duas alternativas de *blockchain*: consórcio e privado. Enquanto o *blockchain* consórcio permite que somente alguns membros da rede tenham acesso à informação, o privado centraliza completamente o poder em uma única organização. Ambos os conceitos vão contra as características iniciais.

3.1.2 Smart Contracts (Contratos Inteligentes)

Segundo Szabo [8], um contrato é um conjunto de promessas que, tradicionalmente, formalizam uma relação. Ao definir um contrato inteligente como um conjunto de cláusulas contratuais que podem ser embutidos em *hardware* e *software*, ele afirma que a capacidade de um *smart contract* vai além do exemplo canônico da *vending machine*, pois sua dinamicidade e proatividade independem de terceiros envolvidos.

Um exemplo que pode facilmente tornar-se realidade na sociedade atual são os contratos inteligentes embutidos no computador de bordo de um carro. Supondo que o carro tenha sido comprado a prazo, o sistema é capaz de interromper a ignição caso identifique que há um atraso no pagamento; da mesma forma, ele é capaz de deletar da memória essa checagem após conferir que todas as parcelas foram quitadas. Szabo [8] afirma que esse meio é muito mais barato e eficiente do que envolver advogados, guinchos, entre outros no processo de tomada no veículo.

Kemmoe et. al [13], citando Szabo, afirmam que os objetivos de um contrato inteligente são os seguintes: observalidade, verificabilidade, privacidade e executoriedade. O princípio da observalidade é a habilidade de observar a performance do contrato, ou de provar uma performance própria para a outra parte envolvida. Szabo [8] ainda cita que áreas como contabilidade têm a preocupação de fazer contratos com empresas que sejam mais visíveis nesse sentido.

O conceito de executoriedade diz que ao executar um contrato inteligente, é entendido que ambas as partes concordaram com as cláusulas e estão cientes de seus deveres, além de que uma vez iniciado, não depende de nenhum terceiro para interromper sua execução. É necessário que ele seja completamente executado para que seja legal, além de que também é preciso levar em conta a jurisdição do local onde as partes se encontram.

A verificabilidade é a capacidade de um juiz verificar a execução, completude ou falha do contrato [8]. Por fim, o conceito de privacidade diz respeito à que somente os participantes do contrato devem ter conhecimento sobre o mesmo.

Segundo Raskin [14], os contratos inteligentes podem ser divididos em dois tipos: fortes (*strong*) e fracos (*weak*). Os fortes são aqueles que depois de executados, possuem altos custos de modificação para quaisquer intervenções legais necessárias. Já os fracos, são aqueles que podem ser facilmente modificados após sua execução.

Os conceitos de *smart contracts* conseguem interagir muito bem com a aplicabilidade do *blockchain*: a permissão de somente-leitura garante a imutabilidade e, consequentemente,segurança das partes envolvidas. Nota-se que quaisquer modificações que precisem ser realizadas implicam na criação de um novo contrato, e não na alteração no já existente na cadeia.

3.1.3 Plataforma Ethereum

Baseado no paradigma do *blockchain* e dos contratos inteligentes, surgiu em 2015 a plataforma Ethereum, com o objetivo de criar um protocolo para o desenvolvimento de aplicações descentralizadas através de uma linguagem de programação *turing-complete* embutida em seu próprio *blockchain* [10], além de possuir sua própria criptomoeda: o Ether. Apesar de se basear nos conceitos do *blockchain*,

Ethereum se denomina como uma máquina de estados distribuída ao invés de um *ledger* distribuído, como no caso de criptomoedas tal qual o Bitcoin [18].

Com os princípios de simplicidade, universalidade, modularidade, agilidade e não-discriminação [10], a plataforma procura dar liberdade aos programadores de desenvolverem livremente contratos inteligentes em diversas linguagens diferentes, mas que são convertidos e lidos pela máquina como códigos binários chamados de "*Ethereum Virtual Machine Code*" ou "EVM *code*", executado pela "*Ethereum Virtual Machine*" (EVM).

A EVM é uma máquina de estados representados por uma estrutura de dados denominada Merkle Patricia Trie, responsável por manter todas as contas da plataforma ligadas por *hashes* de forma que podem ser reduzidas à uma única raiz guardada na cadeia [18]. As transações são instruções assinadas de maneira criptográfica pelas contas participantes e são realizadas através da EVM, possuindo retornos que resultam em dois tipos diferentes [18]:

• Criação de contratos: transações que resultam em um novo contrato, contendo o *bytecode* compilado de um contrato inteligente;

• *Message Calls*: chamadas de funções para um contrato a fim de executar o seu *bytecode* e, consequentemente, aplicando o contrato compilado.

Aplicativos desenvolvidos utilizando a plataforma são chamados de *Decentralized* App (DApp), cujo *back-end*, que consiste em um contrato inteligente [19], é executado em uma rede ponto a ponto e o *front-end* pode ser hospedado em serviços centralizados ou descentralizados. Segundo [15], já existem mais de três mil aplicativos operando desta forma. Em [19], afirma-se que um DApp é composto das seguintes características:

• Descentralizado: funcionam de maneira independente e não podem ser controlados por grupos ou indivíduos. Apesar de ser visto como vantagem, essa descentralização dificulta a manutenção e a atualização de aplicativos já presentes na rede;

• Determinístico: executam as mesmas funções, independente do ambiente;

• Turing Completo: executam qualquer ação, desde que sejam programados para tal;

• Isolados: são executados na máquina virtual da plataforma. Isto impede que quaisquer bugs ou erros de programação impactem diretamente na performance da cadeia.

Os contratos inteligentes podem ser escritos em diversas linguagens que possuam tal finalidade específica, sendo Solidty e Vyper as mais ativas [20]. Para garantir a sustentabilidade da rede bem como incentivar a participação de mineradores, Ethereum utiliza-se do conceito chamado de *gas fee*, que é a aplicação de uma taxa (em Ether) sob qualquer transação para servir como recompensa do minerador responsável pela validação do bloco [21]. O custo do *gas* é proporcional à necessidade de poder

computacional e complexidade do contrato em questão, sendo possível calculá-la antes de realizar o *deploy* para a cadeia.

As instruções de um contrato inteligente são uma série de *opcodes* presentes como instruções da EVM. Segundo [18], os contratos são capazes de executar desde instruções mais simples como XOR, AND, ADD e SUB até instruções que são referentes à manipulação da pilha em *blockchains*, como ADDRESS, BALANCE, KECCAK256, BLOCKHASH dentre outros.

Atualmente, a plataforma está migrando do algoritmo de consenso *Proof of Work* para o *Proof of Stake*, no processo, chamado Eth2 [22] ou Etherium 2.0. Foram consideradas as seguintes problemáticas que levaram a tal decisão:

• Alto custo de energia: o processo de mineração necessita de muita energia, a qual grande parte é desperdiçada [23]. No processo de *Proof of Stake*, os validadores são os nós que possuem maior concentração monetária na rede;

• Altas barreiras de entrada: é necessário possuir muito poder computacional para poder participar na validação dos blocos e ganhar recompensas. No algoritmo do *Proof of Stake* é possível participar com baixo investimento em *hardware*;

• Risco de centralização: no modelo atual, podem existir poucos nós que conseguem competir nas redes, consequentemente, centralizando a validação dos blocos entre si. Porém, de acordo com [24], o *Proof of Stake* também é suscetível à centralização à longo prazo, sendo necessário o desenvolvimento ou adaptação de outro algoritmo que leve esta problemática em consideração.

Há a possibilidade de utilizar a rede Ethereum como base para a criação de uma rede privada, como indicado em [25]. Os nós desta rede privada não se comunicam com a principal, o que permite que sejam aplicadas regras e algoritmos de consenso diferentes dos já existentes. Devido a essa flexibilidade, os Dapps desenvolvidos utilizando a plataforma conseguem variar desde novas criptomoedas até mesmo jogos [26], além de permitir que sejam criados ambientes de teste para o poder computacional de contratos inteligentes.

3.1.4 Blockchain e Smart Contracts na área de saúde

A plataforma Ethereum é a prova de que a implementação de contratos inteligentes no sistema *blockchain* é plausível e funciona. No entanto, segundo Christidis *et al*. [6], ao unir-se com a área de saúde, existem alguns problemas que devem ser resolvidos.

Comparado com um banco de dados centralizado, devido ao seu *modus operandis*, é normal que o *blockchain* seja mais devagar [6]. Além disso, seguindo o seu conceito inicial, todas as transações do *blockchain* devem ser abertas para que os participantes da rede tenham acesso. Nesse cenário, como as

chaves também estão abertas ao público, é possível que algum usuário de má índole consiga rastrear e, através de padrões, identificar um desses participantes.

No entanto, a modernização desse tipo de serviço também traz diversas vantagens. Segundo [16], uma das vantagens atreladas a esse desenvolvimento é de melhor qualidade na prestação do serviço médico e redução de custos para as organizações. No atual estado da arte, *healthcare* é um serviço caro e inacessível para parte da população, principalmente as de países que não possuem um sistema público de saúde. Além disso, permitir que os pacientes decidam quais informações devem ser compartilhadas é um processo de transparência e aumenta a confiabilidade das organizações e seus *stakeholders* [17].

Os registros imutáveis permitem que o rastreio de insumos destinados à fabricação de remédios ou até mesmo a deslocamento entre as fábricas e as distribuidoras seja não somente um impacto positivo para a logística, como também para a área de saúde em geral, podendo diminuir, ou até mesmo futuramente extinguir, a falsificação e desvio indevido de medicamentos, insumos, dentre outros [27] que sejam de vital importância para hospitais e clínicas.

Como referência da aplicação destas tecnologias, há o projeto desenvolvido por [28], que propõe uma prova de conceito relativa ao processo do fluxo completo de vacinação através de contratos inteligentes para registro de clientes, vacinas disponíveis, aplicação e *checkout*.

O trabalho desenvolvido por [29] apresenta um sistema de gerenciamento de prontuários eletrônicos utilizando-se do *blockchain* da plataforma Ethereum como base, propondo uma cadeia privada para uso em sistemas de neurorreabilitação através de um modelo colaborativo que inclui pacientes, empresas de serviços de saúde e instituições de ensino e pesquisa. Neste modelo, os pacientes decidem quais informações querem compartilhar e com quem, realizando o registro de novas sessões à medida que elas forem ocorrendo.

3.2 OBJETIVO

3.2.1 Objetivo Geral

Investigar trabalhos que utilizem contratos inteligentes, baseados no paradigma *blockchain*, em aplicações nas áreas de saúde.

3.2.2 Objetivos específicos

Investigar trabalhos relacionados ao paradigma *blockchain* com relação aos seus conceitos, seu funcionamento, ferramentas, linguagens de desenvolvimento, ambientes e suas aplicações; Investigar

trabalhos relacionados aos contratos inteligentes, em especial na plataforma Ethereum, com relação aos seus conceitos, seu funcionamento, ferramentas, ambientes com e suas aplicações; Investigar trabalhos que mostrem aplicações de contratos inteligentes no paradigma *blockchain* em aplicações nas áreas de fisioterapia/reabilitação;

3.3 MATERIAL E MÉTODOS

Foi realizada uma revisão sistemática da literatura acerca dos temas: *blockchain*, *smart contracts*, *blockchain on smart contracts* e *ethereum*. As pesquisas foram realizadas a partir das seguintes strings de busca: *health data*, *healthcare cryptography*, *blockchain healthcare*, *blockchain data sharing*, *healthcare data consensus*, *smart contracts*, *ethereum* utilizando sites como o IEEE, Google Scholar e ResearchGate para obtenção dos artigos.

Foram inclusos somente artigos pertinentes ao tema geral estudado ou que oferecessem informações técnicas acerca do funcionamento e/ou estado da arte dos sistemas *blockchain*, *healthcare* e plataforma Ethereum. Visto que muitas vezes foram encontrados somente resumos que não explicavam a fundo o funcionamento desses sistemas, materiais web de fontes confiáveis (como o *whitepaper* disponibilizado pela própria Ethereum) foram utilizados como material de apoio para embasar as informações obtidas. Outro fator de inclusão foi que os artigos deveriam possuir acesso gratuito.

Visando um embasamento teórico mais condizente com o estado da arte atual, quaisquer materiais anteriores a 2015 foram descartados. No entanto, o texto escrito por Nick Szabo, o criador do conceito de contratos inteligentes, assim como o *whitepaper* de Satoshi Nakamoto sobre a moeda Bitcoin, ambos datados antes da data de exclusão definida, foram mantidos, visto que esses foram os responsáveis pela criação de dois conceitos estudados nesta pesquisa. Os materiais inclusos foram divididos nas seguintes categorias:

Categoria	**Referências**
Embasamento do conceito *blockchain*	Bitcoin: A Peer-to-Peer Electronic Cash System [1] An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends [3] COMO funciona o Proof of Work na blockchain do Bitcoin [5] Introdução às tecnologias dos blockchains e das criptomoedas [10] BLOCKCHAIN: Prova de Trabalho (POW) x Prova de Participação (POS) [12]

	Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion [23]
Embasamento sobre contratos inteligentes	Blockchains and Smart Contracts for the Internet of Things [6] Smart Contracts: Formalizing and Securing Relationships on Public Networks [8] A Survey on Security Verification of Blockchain Smart Contracts [11] The Law and Legality of Smart Contracts [14]
Explicação sobre a plataforma Ethereum e suas tecnologias	UMA Plataforma para Smart Contracts e Aplicações Descentralizadas da Próxima Geração [9] ETHEREUM VIRTUAL MACHINE (EVM) [18] INTRODUCTION TO DAPPS [19] SMART CONTRACT LANGUAGES [20] GAS AND FEES [21] PROOF-OF-STAKE (POS) [22] e-PoS: Making Proof-of-Stake Decentralized and Fair [24] PRIVATE NETWORKS [25] Which Crypto Projects Are Based on Ethereum? [26]
Blockchain e/ou contratos inteligentes aplicados às áreas da saúde	Using Blockchain for Electronic Health Records [4] Applications of Blockchain Within Healthcare [7] Improving Healthcare Processes with Smart Contracts [16] Dynamically integrating electronic-with personal healthrecords for ad-hoc healthcare quality improvements [17] Blockchain for drug traceability: Architectures and open challenges [27] Modelo de negócio para saúde colaborativa usando smart contracts: caso TokenHealth [28] Blockchain para gerenciamento de prontuários eletrônicos [29]

3.4 RESULTADOS E DISCUSSÃO

Mesmo que os trabalhos relacionados à reabilitação e fisioterapia sejam escassos, analisando os conceitos apresentados nas leituras categorizadas previamente como "*blockchain* e/ou contratos inteligentes aplicados às áreas da saúde", forma-se uma ideia de como seriam os papeis destas tecnologias em um ecossistema similar.

Considerando os estudos até o momento, é plausível admitir que um sistema de *blockchain* integrado juntamente com contratos inteligentes pode ser capaz de proteger os pacientes, visto que

qualquer laudo médico têm a possibilidade de ficar registrado na cadeia e, dependendo da composição do bloco, ser de fácil auditabilidade, podendo facilmente identificar médicos que tenham cometido algum erro procedural e/ou receitado medicamentos e até mesmo tratamento errôneos ou sem base científica para pacientes.

3.4.1 Tecnologias

Inicialmente, assim como proposto por [29], uma rede colaborativa que inclua empresas de saúde juntamente com institutos de ensino e pesquisa seriam os membros ideais para dar início ao ecossistema, visto que o compartilhamento de dados entre si é benéfico para todas as partes envolvidas.

A utilização de uma rede privada baseada em Ethereum 2.0 que utilizasse *Proof of Stake* ou *Proof of Authority* como algoritmos de consenso evitariam a necessidade de membros externos para desempenhar papel de mineradores e também permitiria que as instituições participantes da rede não precisassem desprender de dinheiro ou *hardware* que poderia estar sendo alocado para outra finalidade. Além disso, por ser uma rede privada, os gastos com *gas fee* poderiam ser reduzidos ou eliminados a depender do algoritmo de consenso utilizado. A utilização de uma criptomoeda interna ou a delegação de autoridade para cada instituição caberia à empresa de saúde dona do *blockchain*, de acordo com as necessidades, sem desconsiderar a possibilidade de criar um algoritmo de consenso próprio.

Os blocos seriam compostos por:

• *Timestamp* (data/hora de quando foi gerado o bloco);

• *Previous block hash*;

• *Bits* (tamanho);

• Merkle *root hash*;

• Chave do paciente (identificador que apontasse para uma determinada posição no banco de dados referente ao prontuário eletrônico do paciente);

• Chave do médico (identificador, equivalente ao CRM, que permitisse a identificação do profissional caso houvesse acesso ao banco de dados da instituição).

A composição do bloco foi proposta levando em consideração a auditabilidade como principal fator. No momento de marcação de uma sessão, seria gerado um contrato inteligente para ser ativo nos dias acordados. O paciente receberia um *token* (da mesma forma que ocorre atualmente em alguns planos de saúde) e o contrato mudaria o comportamento baseado em cláusulas relativas à validação deste *token*, podendo conceder acesso único ao prontuário eletrônico do paciente para o médico ou encerrar a consulta caso não fosse validado (dentro de um determinado tempo) ou validado negativamente.

Após as modificações serem salvas, o bloco é criado e enviado para rede para ser validado. Nota-se que o bloco não armazena qualquer dado; ele somente é o registro referente à data/hora aproximados da modificação, bem como paciente destino e o médico origem. Todas as alterações realizadas no prontuário não são refletidas nele.

Ao fim do contrato, o *opcode selfdestruct* é chamado para removê-lo da cadeia, sendo necessário a criação de um contrato novo caso preciso.

3.4.2 Transparência dos dados

Os pacientes devem poder alterar a permissão dos dados a qualquer momento, podendo escolher quais dados desejam compartilhar e quais organizações podem recebê-los. Além disso, é preciso também que as instituições sejam transparentes nas coletas de dados, como reforçado por [17].

3.4.3 Compartilhamento dos dados com instituições externas

O compartilhamento de dados deve ser feito de forma que não identifique os pacientes. Técnicas como anonimização e inserção de ruído podem ser empregadas com este fim. Além disso, é preferível que o acesso aos dados não seja direto no banco de dados que contém os prontuários eletrônicos dos pacientes, mas sim somente aos dados em questão.

3.5 CONCLUSÃO

Blockchain e *Smart Contracts* são tecnologias que datam de mais de uma década. Mesmo havendo casos de implementações com sucesso, como no caso da Estônia, nota-se que somente ao longo dos últimos anos, após a popularização das criptomoedas, começou-se a estudar a integração destas tecnologias em diversas áreas diferentes. No entanto, os estudos direcionados para as áreas de saúde costumam ser proposições de sistemas gerais ou revisões sistemáticas, fazendo com que aplicações mais específicas ainda sejam escassas.

Contudo, nota-se que os benefícios trazidos pela integração dessas tecnologias são bastante claros, sendo um passo importante para modernização dos sistemas em uma era onde o acesso à informação e compartilhamento de dados deve ser transparente.

3.6 REFERÊNCIAS

[1] NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 10 jan. 2021.

[2] S., L. Who is Satoshi Nakamoto? **The Economist**. Disponível em: https://www.economist.com/the-economist-explains/2015/11/02/who-is-satoshi-nakamoto. Acesso em: 10 jan 2021.

[3] ZHENG, Zibin; XIE, Shaoan; DAI, Hongning; CHEN, Xiangping; WANG, Huaimin. **An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends**. In: **2017 IEEE International Congress on Big Data (BigData Congress)**, 2017.

[4] SHAHNAZ, Ayesha; QAMAR, Usman; KHALID, Ayesha. **Using Blockchain for Electronic Health Records**. In: **IEEE Access**, 2019.

[5] COMO funciona o Proof of Work na blockchain do Bitcoin. **Livecoins**. 14 abr. 2018. Disponível em: https://livecoins.com.br/proof-of-work-blockchain-bitcoin/. Acesso em: 11 jan 2021.

[6] KONSTANTINOS, Christidis; DEVETSIKIOTIS, Michael. Blockchains and Smart Contracts for the Internet of Things. **IEEE Access**, vol. 4, pp. 2292-2303, 2016.

[7] BELL, Liam; BUCHANAN, William J; CAMERON, Janathan; LO, Owen. Applications of Blockchain Within Healthcare. **BHTY**, vol. 1, mai. 2018.

[8] SZABO, Nick. Smart Contracts: Formalizing and Securing Relationships on Public Networks. **First Monday**, volume 2, number 9, 1 set. 1997. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/548/469.

[9] UMA Plataforma para Smart Contracts e Aplicações Descentralizadas da Próxima Geração. **Github**. Disponível em: https://github.com/ethereum/wiki/wiki/%5BPortuguese%5D-White-Paper#ethereum. Acesso em: 7 mar. 2021.

[10] CHERVINSKI, João Otávio Massari; KREUTZ, Diego. Introdução às tecnologias dos blockchains e das criptomoedas. **Revista Brasileira de Computação Aplicada**, v. 11, n. 3, p. 12-27, 25 set. 2019.

[11] LIU, Jing; LIU, Zhentian A Survey on Security Verification of Blockchain Smart Contracts. **IEEE Access**, vol. 7, 2019.

[12] BLOCKCHAIN: Prova de Trabalho (POW) x Prova de Participação (POS). **ISI-TICs**. 24 jan. 2019. Disponível em: https://isitics.com/2019/01/24/blockchain-prova-de-trabalho-pow-x-prova-de-participacao-pos/. Acesso em: 7 mar. 2021.

[13] KEMMOE, Victor Youdom; STONE, William; KIM, Jeehyeong; KIM, Daeyoung; SON, Junggab. Recent Advances in Smart Contracts: A Technical Overview and State of the Art. **IEEE Access**, vol. 8, p. 117782-117801, 2020.

[14] RASKIN, Max. The Law and Legality of Smart Contracts. **Georgetown Law Technology Review** 304, 2017.

[15] WHICH Crypto Project are Based on Ethereum? **Coindesk**. Disponível em: https://www.coindesk.com/which-crypto-dapps-are-on-ethereum. Acesso em: 7 mar. 2021.

[16] KORMILTSYN, Aleksandr; UDOKWU, Chibuzor; KARU, Kalev; THANGALIMODZZI, Kondwani; NORTA, Alex. **Improving Healthcare Processes with Smart Contracts**. In: **22nd International Conference on Business Information Systems**, 2019.

[17] KORMILTSYN, Aleksandr; NORTA, Alex. **Dynamically integrating electronic-with personal healthrecords for ad-hoc healthcare quality improvements**. In**: International Conference on Digital Transformation and Global Society**. p. 385–399. Springer, 2017.

[18] ETHEREUM VIRTUAL MACHINE (EVM). **Ethereum**. 13 mai. 2021. Disponível em: https://ethereum.org/en/developers/docs/evm/. Acesso em: 13 jun. 2021.

[19] INTRODUCTIONN TO DAPPS. **Ethereum**. 11 jun. 2021. Disponível em: https://ethereum.org/en/developers/docs/dapps/. Acesso em: 13 jun. 2021.

[20] SMART CONTRACT LANGUAGES. **Ethereum**. 10 mai. 2021. Disponível em: https://ethereum.org/en/developers/docs/smart-contracts/languages/. Acesso: 16 jun. 2021.

[21] GAS AND FEES. **Ethereum**. 22 jun. 2021. Disponível em: https://ethereum.org/en/developers/docs/gas/. Acesso em: 28 jun. 2021.

[22] PROOF-OF-STAKE (POS). **Ethereum**. 15 abr. 2021. Disponível em: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. Acesso em: 01 jul. 2021.

[23] HOUBEN, Robby. SNYERS, Alexander. Policy Department for Economic, Scientific and Quality of Life Policies. **Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion**. Jul. 2018.

[24] SAAD, Muhammad; QIN, Zhan; REN, Kui; NYANG, Daehun; MOHAISEN, David. e-PoS: Making Proof-of-Stake Decentralized and Fair, 2021.

[25] PRIVATE NETWORKS. **Ethereum**. Disponível em: https://geth.ethereum.org/docs/interface/private-network. Acesso em: 05 jul. 2021.

[26] HERTIG, Alyssa. Which Crypto Projects Are Based on Ethereum? **Coindesk**. 23 mar. 2021. Disponível em: https://www.coindesk.com/which-crypto-dapps-are-on-ethereum. Acesso em: 10 jul. 2021.

[27] UDDIN, Mueen; KHALED, Salah; JAYARAMAN, Raja; PESIC, Sasa; ELLAHHAM, Samer. Blockchain for drug traceability: Architectures and open challenges. **Health informatics jornal**, volt 27, 2021.

[28] BRANCO, Vinicius; LIPPERT, Bruno; LUNARDI, Roben Castagna; NUNES, Henry C.; NEU, Charles V.; ZORZO, Avelino F.; PIROLLA, Diego; BERNUCIO, Reider A.; SPACOV, Sérgio. Modelo de negócio para saúde colaborativa usando smart contracts: caso TokenHealth. **Revista Brasileira de Computação Aplicada**, v. 12, n. 1, p. 134-144, 2 abr. 2020.

[29] Viana, Caroline; Brandao, Alexandre; Dias, Diego Roberto; Castellano, Gabriela; Guimaraes, Marcelo. (2020). Blockchain para gerenciamento de prontuários eletrônicos. **RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao**. 1. 177, abr. 2020.