Sharing Health and Wellness Data with Blockchain and Smart Contracts

P. Rangel, and J. Kleinschmidt

***Abstract*—Increased longevity and people's concern about aging with quality has led to increased health and wellness data. Much of the data is not interoperable because of its divergent structures and semantics, being little used and little protected. Existing standards are complex and lack the adherence of the agents involved to ensure their application. Blockchain technology offers alternatives to unify the standards and their application by consensus algorithm, which considers the validation and secrecy in the insertion of the blocks of transactions in the chain. However, smart contracts can ensure secrecy and the rules of data sharing in blocks in the chain. In this paper, we propose a blockchain architecture with a consensus algorithm that considers data collected in the health and wellness ecosystem, including those obtained by IoT devices and persisted in middleware platforms. It is intended that this architecture be able to answer the questions and establish the concepts for the full and secure sharing of health and wellness data.**

***Index Terms*—Blockchain, Health, Internet of Things, Middleware, Smart contracts, Wellness.**

I. Introdução

A longevidade da população apresentou um forte crescimento nas últimas décadas e mantém esta tendência [1], o que é notado pelos adultos jovens e de meia idade com a percepção da importância em ter um estilo de vida saudável, na busca da saúde do corpo e da mente, preparando-se para o envelhecimento de forma plena e ativa [2].

Assim, ao longo do tempo cada vez mais dados sobre bem-estar e saúde são coletados por hospitais, clínicas, médicos, etc., somando-se aos que são coletados em tempo real com o uso de dispositivos pessoais que monitoram medidas ambientais e biométricas em atividades físicas, aumentando o volume e a sua importância. Também se nota que parte importante deles, em razão da sua dispersão, estruturas de dados incompatíveis e semântica divergente, são pouco utilizados e até mesmo perdidos, recebendo pouca ou nenhuma proteção [3].

Assim, depara-se com o desafio de torná-los interoperáveis, seguros, sigilosos, e disponíveis em rede de alta disponibilidade, para que se transformem em informação e conhecimento, beneficiando o indivíduo e a sociedade.

Paulo S. R. Garcia e João H. Kleinschmidt, Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, Universidade Federal do ABC, Santo André - Brasil. E-mail: paulo.rangel@ufabc.edu.br; joao.kleinschmidt@ufabc.edu.br.

Este trabalho propõe a *blockchain*, tecnologia viabilizadora das criptomoedas [4] [5], para o compartilhamento de dados de saúde e bem-estar em rede *peer-to-peer* de alta disponibilidade, escalabilidade e resiliência.

A tecnologia *blockchain* se refere a um livro distribuído de registro de transações agrupadas em blocos organizados em uma cadeia. Os blocos inseridos na cadeia são imutáveis, pois cada bloco contém um *hash* de seu conteúdo, que permite verificar a integridade das suas transações. Além disso, o *hash* de um bloco depende do *hash* do bloco anterior, garantindo sua imutabilidade, já que mudar o *hash* de qualquer bloco n - i também mudaria o *hash* do bloco n.

Uma *blockchain* dispensa uma autoridade central para garantir a validade dos novos blocos. Para isso, a *blockchain* completa é distribuída para todos os nós que participam da rede e através de um algoritmo de consenso a validade dos novos blocos de transações é verificada pelos nós ativos da rede.

Os mineradores são os nós responsáveis por formar blocos e inseri-los na *blockchain*. É por eles que a estratégia de consenso acontece, em geral por um protocolo de incentivo. Em *bitcoin*, p. ex., são incentivados pela cobrança de taxas de transação e por uma recompensa pela inclusão do bloco na *blockchain*. Em geral, deve existir um incentivo para que construam blocos válidos, o que leva a rede ao consenso.

Este trabalho apresenta uma proposta de arquitetura que considera desde a coleta de dados pessoais de saúde gerados pelos próprios usuários aos dados gerados pelos atores do ecossistema de saúde, como p. ex., hospitais e clínicas, as questões sobre os dados quanto a sua interoperabilidade, unificando a semântica e estruturas, o seu compartilhamento, a sua segurança e criptografia, além da identidade e compartilhamento de chaves,.

E por fim que apenas as partes autorizadas tenham acesso aos dados após incluídos na cadeia de blocos. Ainda, assegurando que mineradores íntegros sejam eleitos para incluir blocos, garantindo o consenso e a segurança da rede.

Neste contexto, os contratos inteligentes (do inglês *smart contracts*) [5], devem assegurar que apenas os usuários concederão acesso aos seus dados, impedindo o repúdio ou o não cumprimento de qualquer cláusula contratada. Por fim a integração com *middlewares*, possibilitando que dados de bem-estar e saúde coletados pelos pacientes e por dispositivos IoT (*Internet of Things*) sejam persistidos e inseridos na cadeia.

O artigo está estruturado da seguinte forma: a seção II apresenta outros trabalhos relacionados aos temas desta proposta, na seção III, abordam-se questões que envolvem interoperabilidade, padrões e legislações para a coleta de dados no ecossistema de saúde e bem-estar. Na seção IV apresenta-se

a proposta de arquitetura, na seção V analisam-se os benefícios potenciais, trazendo as conclusões e propostas de trabalhos futuros.

II. Trabalhos Relacionados

A aplicação de *blockchain* como tecnologia de suporte para o compartilhamento e gerenciamento de dados de saúde e bem-estar está em discussão pela comunidade científica para diversas aplicações.

Mikula e Jacobsen[21] a abordam propondo como solução para um sistema descentralizado de gerenciamento de identidade e acesso, explorando uma *blockchain* baseada no *Hyperledger Fabric* para as operações básicas de autenticação e autorização como registro, *login*, concessão / revogação de permissões e atualizações no sistema, desenvolvendo uma prova de conceito a partir do universo de médicos da Dinamarca.

No compartilhamento de dados, Jiang et al [22], discutem uma plataforma *blockchain* para o compartilhamento de dados de saúde, propondo duas cadeias de blocos onde os dados coletados pelos atores do sistema de saúde (p. ex., Hospitais e Clinicas) estarão separados dos dados pessoais coletados pelos próprios pacientes, p. ex., por dispositivos IoT e/ou vestíveis.

Espósito et Al [23], apresentam um modelo para o compartilhamento de dados em nuvem com a cadeia de blocos recebendo URL's apontando para onde os dados estarão armazenados e não os dados propriamente. Isto em razão das informações poderem estar armazenadas em países ou blocos de países como os EUA ou a União Europeia que possuem legislações distintas sobre a Proteção de Dados Pessoais, p. ex., no Brasil a Lei Geral de Proteção de Dados número 13.709/18 e o artigo 17º do Regulamento Geral de Proteção de Dados da União Europeia estabelecem o direito do cidadão em alterar ou solicitar que seus dados sejam apagados, o que para dados incluídos em uma cadeia de blocos não é possível. Além disso, dados como exames baseados em imagens, de forma geral, representam um grande volume de informação limitando a sua inserção em cadeias de blocos.

Uma preocupação importante na sociedade é sobre a economia circular, que no caso do fornecimento de serviços, busca que sejam eficientes, rentáveis e sustentáveis, ainda mais quando se trata de saúde, frequentemente custeados por recursos públicos. Para alcançar estes objetivos, Alexaki, Alexandris e Petroulakis [24] propõem, através da tecnologia *blockchain*, a criação de um ciclo de cuidados integrado, descentralizado e holístico, onde, p. ex., a disponibilidade das informações de diagnósticos e exames sejam compartilhadas entre os diversos atores, evitando assim, entre outras coisas, a perda de informações e a repetição de exames e diagnósticos.

Peterson [8] propõe um novo algoritmo de consenso, a *Prova de Interoperabilidade* (do inglês *Proof of Interoperability*) a partir de uma fonte centralizada de padrões e semântica. Shrier [3] discute um protótipo do sistema ENIGMA / OPAL do MIT *Media Lab* que utiliza uma camada de criptografia baseada em técnica conhecida como criptografia segura em computação distribuída (do inglês *Cryptography Secure Multi-Party Computation* - MPC) [20]. Ekblam [11] propõe o compartilhamento de dados de registros eletrônicos de saúde (do inglês *Electronic Health Records* - *EHRs*) através do modelo proposto por Zyskind [19] de privacidade descentralizada adotando *blockchain* para proteger dados pessoais, baseado também no Projeto ENIGMA. Enquanto Peterson [8] aborda as questões de interoperabilidade e algoritmo de consenso, Shrier [3] e Ekblam [11] abordam as questões da privacidade, proteção e sigilo dos dados.

Neste trabalho propõem-se uma arquitetura que cubra um espectro mais amplo que os estudos mencionados, indo desde a coleta de dados pessoais gerados pelos usuários e pelos atores do ecossistema de saúde, tratando as questões de semântica e interoperabilidade, segurança, criptografia e acessos chegando até a inserção de registros em blocos dentro de uma *Blockchain*.

III. Coleta de Dados

Um aspecto relevante sobre a coleta de dados de saúde é o reconhecimento do conceito que o indivíduo, mesmo sem a posse e guarda de seus dados pessoais, tem o direito de privacidade e sigilo, sendo o único detentor dos direitos de propriedade e arbítrio sobre eles. Vários países possuem legislações consolidadas para a proteção de dados pessoais o que delimita os direitos e obrigações dos indivíduos e das entidades que detêm a posse das informações, como os EUA com a *HIPPA - Health Insurance Portability and Accountability Act of 1996* [13] e HITECH - *Health Information Technology for Economic and Clinical Health Act* [7], e a Comunidade Europeia com o GDPR (*General Data Protection Regulation*) [15]. No Brasil, legislações diferentes buscam dar garantias à privacidade. Podem ser citadas a Lei de Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet, além de alguns dispositivos constitucionais genéricos, como os artigos 5º, 10º e 12º da Constituição Federal [14]. Podem-se acrescentar as Normas de Conduta do Conselho Federal de Medicina e em especial a Lei Geral de Proteção de Dados 13708/18 de 14 de agosto de 2018 com entrada em vigor prevista para agosto de 2020 [16].

Outro aspecto importante em relação a legislação brasileira é a instituição do Cartão Nacional de Saúde [12] como o identificador universal dos pacientes do SUS (Sistema Único de Saúde), além do estabelecimento de uso do padrão *IHE-PIX* pelo Ministério da Saúde [6].

Na outra ponta desta relação existem os diversos atores do ecossistema de saúde, que coletam e detêm informações de seus usuários, e que tem a obrigação de proteger e armazenar tais dados, disponibilizando-os quando necessário a interessados previamente autorizados pelo indivíduo detentor do direito de propriedade e arbítrio sobre eles.

Espera-se que os dados sejam compartilhados e que todos possam compreender a sua estrutura e semântica, com a interoperabilidade que permita os melhores usos em ações e serviços de bem-estar e saúde para a população, não apenas no plano individual, mas também nas que envolvem ações públicas como em pesquisas cientificas, políticas e alocações de recursos públicos de forma eficiente e transparente.

Assim, um dos pilares que podem apoiar o indivíduo, a sociedade e os governos, a atender tais necessidades será o compartilhamento com interoperabilidade das informações de saúde e bem-estar e assim, depara-se com o desafio de como compartilhá-los, preservando-os e mantendo-os privados, seguros e sigilosos em uma rede única de alta disponibilidade,

garantindo os direitos de propriedade e arbítrio do indivíduo sobre seus dados pessoais.

Foram adotadas medidas importantes no Brasil [6] e nos EUA [7], para adoção de padrões de interoperabilidade; no Brasil com o *openEHR* (*Open Eletronic Health Records*) e nos EUA, com o FHIR (*Fast Healthcare Interoperability Resources*). Porém existem outros formatos para garantir a interoperabilidade completa, conforme portaria do Ministério da Saúde [6] que regulamenta os padrões de interoperabilidade e informação em saúde para sistemas de informação. A partir disso, a *blockchain* surge como uma tecnologia viabilizadora de solução para o compartilhamento de dados.

Desde o surgimento do *Bitcoin Core* como software aberto, outras plataformas também *open source* surgiram. Algumas são derivadas do próprio *Bitcoin Core*, e outras de novos desenvolvimentos, apresentando novas características úteis para aplicações de uso geral, além das transações monetárias. Dentre estas características se pode destacar ser Turing-completo, possuir contratos inteligentes, adotar outros algoritmos de consenso além da Prova de Trabalho e na natureza de sua rede: pública, privada ou híbrida.

Para que o compartilhamento seja possível através de uma rede distribuída *peer-to-peer*, utilizando-se *blockchain*, pretende-se abordar o tema sob os seguintes aspectos:

a) *Identidade dos usuários* – compatibilizar o cadastro único de pacientes previsto na Norma Brasileira com o conceito de ausência de terceiros na relação entre as partes, mitigando o ponto único de falhas dessa centralização.
b) *Interoperabilidade* - compatibilizar as estruturas de dados e unificar a semântica dos dados, garantindo a interoperabilidade por padrões únicos de estrutura e semântica, sem que isso crie um ponto único de falhas.
c) *Segurança dos dados* – garantir o consenso e integridade da *blockchain*, proporcionando garantias criptográficas no compartilhamento de dados com privacidade e que apenas as partes autorizadas tenham acesso a eles.
d) *Inserção de dados na cadeia* – a partir de protocolo de incentivo, estimular mineradores íntegros a formar e incluir blocos na cadeia, buscando o consenso e segurança da rede.
e) *Contratos inteligentes* – garantir que apenas os pacientes ou usuários terão o poder de conceder acesso aos seus dados pessoais, garantindo o contratado.
f) *Integração com middlewares* - Integrar dados coletados em dispositivos IoT na *blockchain* de saúde e bem-estar.

IV. Proposta de Arquitetura

A visão geral da arquitetura proposta de *blockchain* para saúde e bem-estar está representada na Fig. 1, em que se apresentam os atores e suas interações até os dados serem inseridos na *blockchain*.

Os diferentes atores são representados e coletam dados de exames clínicos, exames de imagens, de sensores e medidores biométricos, etc., persistindo-os em sistemas próprios em suas redes, com os dados fluindo apenas intrarede, que em geral possuem pouco ou nenhum nível de confiança com os sistemas e redes dos outros atores. Na Fig. 1 foi feita uma distinção entre a coleta e uso de dados no ecossistema de saúde e bem-estar (*Health Ecosystem*) e no ambiente doméstico (*Homecare*).

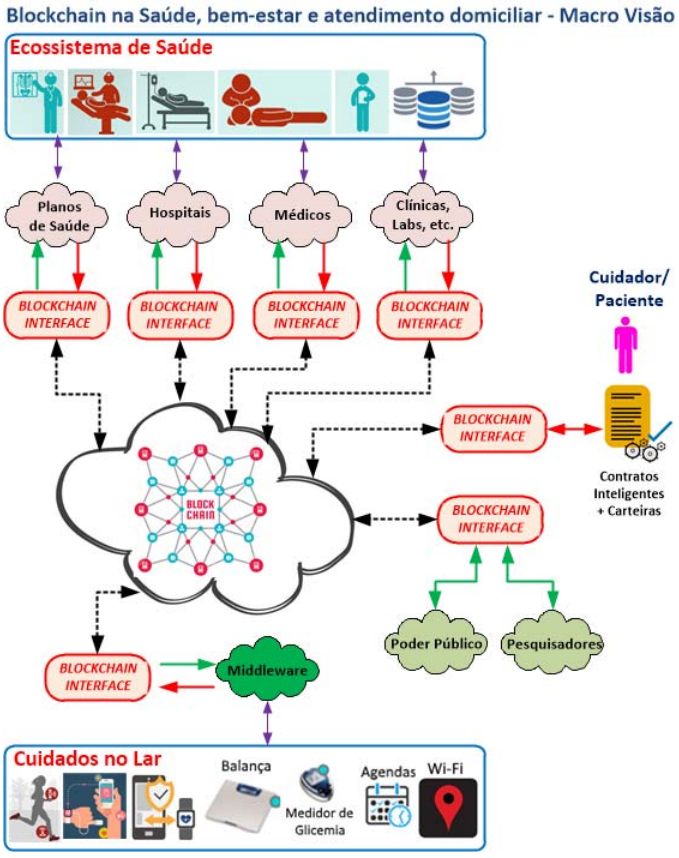

Fig. 1. Visão geral da arquitetura de *blockhain* para saúde e bem-estar.

O ecossistema de saúde e bem-estar é formado por laboratórios, planos de saúde, clínicas, médicos, governos, pesquisadores, hospitais, etc., que em geral possuem infraestrutura de TI (*software* e *hardware*) integrada para a coleta, tratamento, persistência, uso e gestão dos dados.

Já o ambiente doméstico é formado por sensores e atuadores que captam dados não críticos, porém relevantes por demonstrarem comportamentos e tendências. Além disso, em geral não dispõe de infraestrutura integrada de TI, limitando-se em geral a dispositivos não integrados, como aplicativos em *smartphones* se comunicando em curtas distâncias, via *Bluetooth*, por exemplo.

Outro grupo importante no contexto de atores são os pacientes, detentores do direito dos seus dados pessoais, podendo dar acesso a outros interessados no ecossistema.

Considerando o ecossistema de saúde e bem-estar, percebe-se que cada ator opera com infraestrutura de TI única. Logo, a integração com a *blockchain* ocorrerá por uma interface padrão em um serviço disponível na rede interna, que deverá dispor de APIs que a partir de regras e padrões pré-determinados, receberá dados e comandos para interagir com a cadeia de blocos: inserir transações, consultar dados, etc.

Esta interface padrão está representada na Fig. 1 como *Blockchain Interface.* Está presente nas interações de qualquer um dos atores com a cadeia de blocos. Na Fig. 2 é apresentada a visão mais detalhada da *Blockchain Interface.*

A *Blockchain Interface* propõe 5 camadas de funções para tratamento das interações com a *blockchain*. A primeira camada é a *Data Processing* onde há o processamento dos dados recebidos através das APIs, realizando a validação inicial de

funções solicitadas e parâmetros enviados. Ao final retornará o status para o sistema que chamou a função, como p. ex., OK na inserção no bloco se a operação for bem-sucedida, caso contrário, o erro que explique por que não o foi.

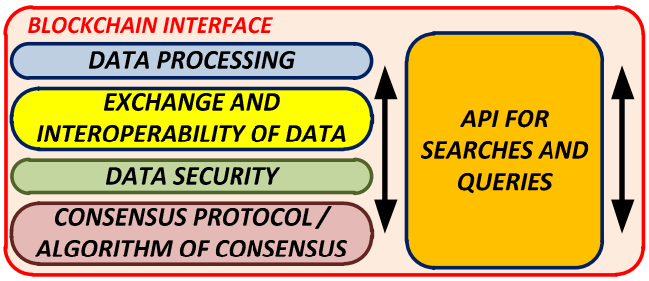

Fig. 2. Visão da *Blockchain Interface*.

A camada seguinte recebe os dados validados da *Data Processing* e tratará a interoperabilidade e troca de dados, validando os padrões de estrutura e semântica dos dados recebidos da camada anterior. Com a interoperabilidade dos dados constatada, eles são enviados para a próxima camada, do contrário é enviado a camada anterior o erro identificado.

A terceira camada, *Data Security*, trata de funcionalidades de criptografia, que permitem preparar os dados para a camada seguinte, *Algorithm of Consensus,* que mediará o processo de inserção da transação em um bloco na cadeia.

Por fim a camada *API for Searches and Queries* realiza na cadeia de blocos as pesquisas e consultas em transações daquela origem ou sumarizadas.

A. *Identidade dos Usuários*

Nas moedas digitais, a identificação dos usuários na *blockchain* se dá por chaves assimétricas geradas por *softwares* conhecidos como carteiras digitais (*digital wallets*), sem a necessidade de intermediação de terceiros. Tem como características impedir a recuperação da chave privada por terceiros em caso de perda e não criar banco de dados central que associe a chave pública a uma pessoa ou organização.

No ecossistema de saúde e bem-estar, os geradores de informações, em geral, serão os atores que possuem bancos de dados de pacientes em seus sistemas privados. No Brasil, o Governo Federal através de portarias do Ministério da Saúde [6] [12] estabelece a identidade universal para atendimento aos pacientes do Sistema Único de Saúde (SUS), também gerando um banco de dados central dos segurados.

Diante da necessidade do compartilhamento da chave pública entre estes atores, na arquitetura proposta as chaves assimétricas podem ser geradas pelo usuário de forma análoga a das moedas digitais, com o paciente fornecendo a cada ator a sua chave pública no momento de seu cadastramento como paciente naquela entidade. Isto pode ser feito, por exemplo, junto ao Governo Federal quando a inclusão do paciente no Cadastro Universal de Pacientes, garantindo assim que apenas o usuário conhece sua chave privada.

B. *Interoperabilidade*

Um caminho para garantir a interoperabilidade está na definição do algoritmo de consenso. Peterson [8] define um novo algoritmo chamado de Prova de Interoperabilidade (*PoI*) que propõe garantir que as transações recebidas são interoperáveis em relação a um determinado padrão de restrições estruturais e semânticas usando padrões pré-estabelecidos em normatizações como as adotadas pelo Ministério da Saúde Brasileiro [6]. A Prova de Interoperabilidade em relação a Prova de Trabalho aproveita o esforço computacional e a energia despendidos para garantir a interoperabilidade das transações.

Outro caminho pela interoperabilidade é explorar recursos de programação dos contratos inteligentes e fazê-lo de forma customizada independentemente do algoritmo de consenso adotado, criando as funções necessárias para verificá-la, por hipótese, no momento da inclusão da transação.

Outra questão relevante é como disponibilizar estes padrões estruturais e semânticos para que todos os nós tenham acesso a eles. Peterson [8] propõe um modelo de repositório central, citando como alternativa a *Value Set Authority Center* (VSAC) [9], ontologia de termos acessado pela *Unified Medical Language System* (UMLS), disponibilizado pela *U.S. National Library of Medicine.*

A proposta de um repositório central traz a questão do ponto único de falhas, não em relação ao comprometimento dos dados da *blockchain*, pois são disponíveis na rede, mas em razão do comprometimento, p. ex., por indisponibilidade do repositório central (VSAC). Isto teria impacto imediato na verificação das informações e, por conseguinte na inclusão de novos blocos na *blockchain,* caracterizando um ataque de negação de serviços.

Nesta proposta pretende-se uma alternativa distribuída para o repositório de padrões de estrutura de dados e semântica. Uma possibilidade é a inclusão dos padrões na *blockchain* como se fossem transações. Outra alternativa é estarem em uma estrutura *blockchain* separada da *blockchain* de dados coletados, mas dentro do contexto de armazenamento dos nós mineradores. Assim, nas duas alternativas, as manutenções (inclusões e alterações) das informações, seriam a partir de APIs das movimentações em um repositório de dados central (VSAC), porém dispensaria que ele estivesse *on-line*, eliminando o ponto único de falhas e ataques de negação de serviços.

C. *Segurança e Privacidade*

Um aspecto importante em transações na *blockchain* de moedas digitais é que não são criptografadas. Assim, se o proprietário de uma chave pública é conhecido, podem-se conhecer todas as suas transações ao longo do tempo. Como os atores do ecossistema de saúde formam bancos de dados que associam os pacientes as suas chaves públicas, é indispensável que existam garantias criptográficas em relação a privacidade das transações.

A questão é como criptografar as transações nos blocos da *blockchain* e mesmo assim permitir que pesquisadores tenham acesso a dados anônimos para seus trabalhos. Em princípio todos os dados críticos e do *payload* devem ser criptografados pelo nodo origem. Os problemas começam com a definição sobre como eleger o minerador, como obter a garantia da interoperabilidade com a criptografia, e qual chave usar e como ela seria trocada entre as partes e quais seriam os nós que teriam acesso ao conteúdo plano da transação [10].

Como a prova de interoperabilidade será realizada pelo minerador, ele terá acesso ao conteúdo plano da transação para validá-la, assim, além dele também o nó origem e o paciente

envolvido na transação deverão conhecer o seu conteúdo, ninguém mais, a não ser que autorizado pelo paciente.

Para que isso ocorra, a transação será enviada, assinada pelo nó origem, ao minerador, criptografada com a chave pública do mesmo, garantindo que só ele acessará o conteúdo. Após receber a transação e decodificá-la com sua chave privada, o minerador realizará a Prova de Interoperabilidade, gerando uma chave simétrica para cada transação, com a qual criptografará o conteúdo da transação recebida.

Esta chave única será criptografada com a chave pública do nó origem e gravada em atributo na transação dentro do bloco. O mesmo se repetirá com a chave pública do paciente, gravando o resultado em outro atributo. Desta forma garante-se que, além do minerador, apenas o nó origem e o paciente terão acesso ao conteúdo quando ela estiver gravada no bloco como pode ser observado na Fig. 3.

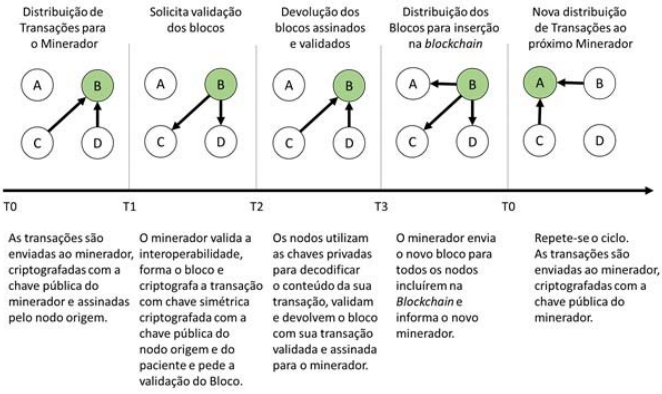

Fig. 3. Fluxo para troca segura de chaves.

A vantagem deste processo é que as chaves simétricas são específicas da transação; se uma dessas chaves for comprometida, o atacante acessará apenas aquela transação. Além disso, garante que os acessos autorizados por contratos inteligentes serão limitados ao que foi estabelecido.

Um dos pontos de risco é a perda ou comprometimento da chave privada do paciente, o que acarretaria a perda do acesso aos dados ou na quebra do seu sigilo, o que é um risco também presente nas *blockchains* de moedas digitais. Outro ponto, é que em dados compartilhados com terceiros, perde-se o controle de como serão tratados dali em diante.

Para que pesquisadores tenham acesso ao conteúdo de transações na *blockchain*, eles precisam estar abertos, porém anônimos, de forma que não se possa associá-los a pacientes.

Esses compartilhamentos podem trabalhar com duas abordagens que não se excluem: a primeira trata da adoção de protocolo baseado em criptografia segura por computação distribuída (do inglês *Cryptography Secure Multi-Party Computation* - MPC), implementado no protocolo *enigma* [20]. Este protocolo permite *queries* genéricas usando poder computacional de nós da rede no qual cada nó acessa um fragmento da informação, que isoladamente não tem significado, processando e compartilhando o resultado com os outros nós de forma que o processamento total aconteça sem que os nós envolvidos tenha acesso completo à informação, garantindo a sua privacidade.

A segunda abordagem envolve a criação de transações de sumarização dos dados de cada bloco a partir de resumos enviados ao nó minerador por cada nó origem das transações naquele bloco. Estas transações resumos trariam como vantagem não utilizar o poder computacional dos nós da rede para obter as informações sumarizadas, porém limitariam as possibilidades de *queries*. As transações sumarizadas também contribuiriam no consenso e validação dos novos blocos como será descrito na próxima subseção.

D. Inserção de Dados e Algoritmo de Consenso

A inserção de dados na *blockchain* (ou mineração) envolve o algoritmo de consenso e como se elege o minerador que incluirá seu bloco na cadeia. No algoritmo de *prova de trabalho* será aquele com maior poder computacional, o que primeiro resolver o desafio matemático. Na *prova de participação*, será aquele que possui o maior saldo médio diário de moedas [17] [18] e na *prova de atividade*, é considerada uma ponderação do saldo médio diário de moedas com a quantidade de transações que o nó efetuou ao longo do tempo que caracterizam sua participação e atividade na rede.

Na *prova de interoperabilidade*, a eleição do próximo minerador se dá por algoritmo que considera um número aleatório enviado pelos nós que participaram na formação do bloco atual. Isto determinará o resultado que corresponderá ao nó eleito e ativo cujo número for mais próximo desse resultado e que tenha certa quantidade de *tokens* que comprovem a sua participação e atividade na rede [8] [11]. Com o minerador eleito, todos os nós com transações a inserir podem enviá-las sem *broadcasting* na rede, assim economizando banda, processamento e energia.

Os protocolos de incentivos nas criptomoedas buscam atrair a participação de mineradores íntegros na rede. Em *Bitcoin* ou *Ethereum*, a gênesis da moeda digital somada as taxas das transações funcionam como atrativo. Nesta arquitetura pode-se adotar um *token* que teria sua gênese na mineração das transações e blocos. Eles seriam trocados pela pesquisa em dados anônimos e pelo uso da infraestrutura e poder computacional da rede, sendo consumidos como taxas de serviços e execução ao longo do tempo, de forma análoga ao *Ethereum Gas* [5], evitando ataques de *loop infinito* e remunerando o poder computacional utilizado dos nós da rede.

Todo nó participante da rede, utilizando a camada *Blockchain Interface*, será um minerador, gerando os *tokens* que lhe darão importância na participação da rede e que serão consumidos por ele ou transacionados com pesquisadores para que os consumam em suas pesquisas.

O processo de inserção de dados na cadeia acontece em estágios adaptados do proposto por Peterson [8]. Em *bitcoin*, as inserções de blocos têm um tempo certo que está relacionado a dificuldade de cálculo do desafio matemático, que por sua vez está vinculado ao tempo de gênesis das novas moedas. Nesta arquitetura o ciclo de tempo, também determinado, permitirá o processo completo de coleta, formação do bloco, validação, eleição e propagação do bloco e do próximo minerador eleito conforme Fig. 4.

Como é possível observar na Fig. 4, no momento T0 inicia-se a coleta das transações e os nós origens enviam as transações assinadas bem como o resumo assinado do que foi enviado para ser utilizado pelo minerador na sumarização do bloco.

No momento T1, após receber as transações, o minerador valida a interoperabilidade e os resumos, criptografando as

transações com chave simétrica, única para cada transação, e com os resumos validados faz e inclui no bloco uma sumarização geral, assinando e enviando o novo bloco, junto com os resumos parciais de cada origem aos nós participantes para que validem e assinem o bloco.

No momento T2, com o novo bloco e os resumos assinados, cada nó valida suas transações e a sumarização geral, podendo validar o bloco pelos resumos mesmo sem conhecer todas as transações. Com isso enviam a confirmação do bloco ao minerador, junto com o *token* e o número aleatório para a eleição do próximo minerador.

No momento T3, o minerador recebe as confirmações e os *tokens*, determina e confirma o próximo minerador, fazendo um *broadcasting* na rede informando o novo bloco a ser inserido por todos e a identidade do próximo nó minerador junto com os *tokens* que o elegeram para validação da rede.

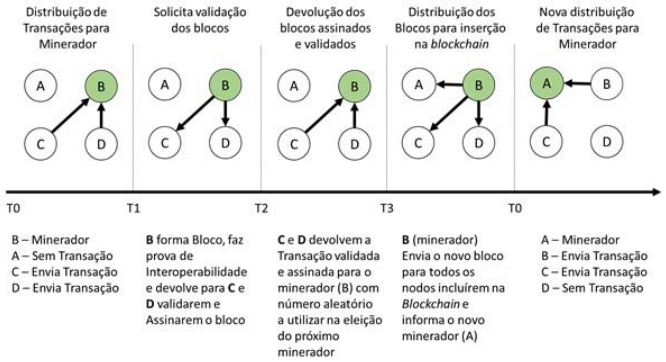

Fig. 4. Fases para inserção de blocos na cadeia.

Com o novo minerador definido, a rede volta ao momento T0, reiniciando-se o fluxo de inserção de blocos na cadeia. Percebe-se que do início do momento T1 até o final do momento T3, todos devem aguardar a definição do próximo minerador para só então enviar as transações que tiverem.

Uma questão importante relacionada a inserção e persistência dos dados é a que envolve a legislação local do nó de origem e dos nós mineradores. Dados de um paciente, por exemplo, da União Europeia, caso solicitado, teriam que ser excluídos ou modificados, porém dentro de uma cadeia de blocos isso não é possível. Uma das alternativas em avaliação é a proposta por Esposito et Al [23] de manter-se na *blockchain* não o dado em si, mas sim a URL (do inglês *Uniform Resource Locator*) de onde o dado pode ser obtido, bem como o *Hash* da informação original de tal maneira que poder-se-á confirmar que o dado original não sofreu nenhuma alteração quando consultado no futuro, e em caso de exclusão ou alteração teríamos a inserção de uma nova transação com a nova condição, informando o novo *hash* ou nova URL sem prejuízo da construção dos blocos anteriores da cadeia.

E. Contratos Inteligentes

Os contratos inteligentes são inseridos na *blockchain* como transações, garantindo sua validade e auditabilidade. Nesta proposta, deverão atender ao compartilhamento de dados, as transações de transferências de *tokens* entre usuários e o compartilhamento de dados.

No compartilhamento de dados, os contratos inteligentes devem garantir que a autorização do paciente seja codificada e executável, como um paciente que deseja que um médico acesse seus exames laboratoriais específicos, ou a partir de uma determinada data e apenas durante certo intervalo de tempo. Por fim as transações de *tokens* devem ser regidas de forma análoga a das criptomoedas, respeitando-se sempre a manutenção de saldo para uso como *Gas* e o impacto que a redução de saldo de *tokens* trará na avaliação de importância do nó no momento da escolha do minerador.

Outro ponto importante é quanto a usabilidade dos contratos inteligentes pelos usuários. Considerando que as situações previstas de contratos inteligentes são bem definidas, pretende-se neste modelo um tipo de aplicação que integre as seguintes funcionalidades: carteira digital para gerar e proteger as chaves assimétricas do usuário, interface amigável para emissão de contratos inteligentes e a *Blockchain Interface.*

F. Integração com Middlewares

A Internet das Coisas tem trazido várias inovações para a área de saúde e bem-estar. Pessoas e objetos passam a portar sensores e atuadores que se comunicam e enviam medições biométricas, ambientais, de estado, e até decidindo ações autonomamente.

Como apresentado na Fig. 5, tais dispositivos geram dados que junto com as novas tecnologias de comunicações de curtas e longas distâncias, como as WPANs (*Wireless Personal Area Network*), WLANs (*Wireless Local Area Network*) e LPWANs (*Low Power Wide Area Network*), possibilitam que as comunicações aconteçam em qualquer lugar ou momento, gerando dados que inseridos na *blockchain*, tem potencial de melhorar a qualidade de vida dos usuários e reduzir os custos de tratamentos da saúde.

Além disso, a disponibilidade de componentes eletrônicos, como microcontroladores, sensores, atuadores e módulos de comunicação de baixo custo com programação de baixa complexidade, mas eficientes, permitem o desenvolvimento de dispositivos personalizados, de baixo custo, integráveis a uma plataforma de *middleware.* Nota-se na Fig. 5, que o *middleware* pode ser dividido em três módulos: *Broker* MQTT, *Blockchain Interface* e *Homecare functionalities*. O MQTT (*Message Queuing Telemetry Transport*) é um protocolo de aplicação comumente adotado em IoT.

O *Broker* MQTT é responsável por autenticar os dispositivos, pelo recebimento dos dados transmitidos, e por sua publicação para consumo do *Middleware*. A *Blockchain Interface* disponibiliza os dados em transações para inserção em blocos na *blockchain*. Por fim o módulo *Homecare functionalities*, dividido em sub-módulos:

- *Device Management* – Interface de gerenciamento dos dispositivos, para cadastrá-los, sendo focado nos atributos cadastrais e características dos dispositivos.
- *Connecting Devices* – Interface para consultar status dos dispositivos, atribuir ID e chave de autenticação. Focado nos atributos de conexão e atuação dos dispositivos.
- *Security* – Faz o processo de autenticação do dispositivo para conectar ao *Middleware* (*Broker* MQTT), criptografia e decriptografia necessárias, seguindo o configurado no módulo *Connecting Devices.*
- *Data Processing* – Tratará o dado recebido, acionando a criptografia, a conversão dos dados e sua validação,

executando gatilhos e persistindo as informações em banco de dados.

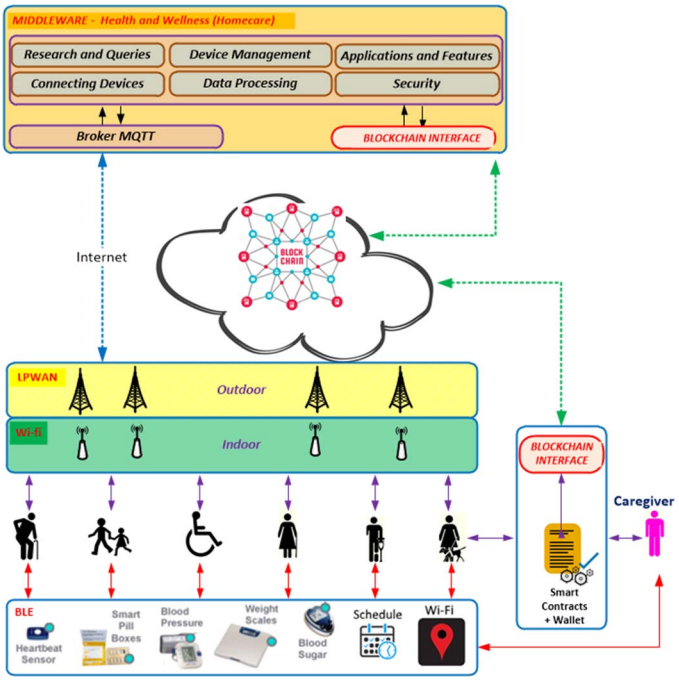

Fig. 5. Integração middleware IoT com blockchain.

- *Research and Queries* – Permite a pesquisa e consulta do estado atual dos dispositivos e sua série histórica.
- *Applications and Features* – Funcionalidades para o paciente e seus cuidadores. Pode registrar agendas de consultas, medicamentos receitados com a frequência e dosagem, histórico sobre consultas, profissionais, etc.

V. Conclusão

O compartilhamento dos dados de saúde e bem-estar permitem grandes benefícios, abrindo possibilidades de aplicação em áreas como aprendizado de máquinas, inteligência artificial, visualização de dados e integração entre *blockchains* distintas. Sob a perspectiva dos usuários, sejam pacientes, cuidadores, etc., se pode destacar os seguintes benefícios:

- Dispensa organizar e manter cópias de exames, receitas, etc., para apresentar a outros profissionais de saúde. Eles estarão organizados e acessíveis, bastando dar acesso pelo tempo e nos registros necessários.
- Dados corretos farão que diagnósticos e tratamentos sejam proativos, assertivos e efetivos, melhorando o atendimento e a qualidade de vida do usuário.

Na perspectiva dos provedores de saúde e bem-estar, os benefícios potenciais seriam os seguintes:

- A colaboração na coleta e compartilhamento de dados com *blockchain* simplificaria a troca de informações;
- Não haveria a disputa por vantagem competitiva baseada na posse de dados, mas sim em métricas de qualidade dos cuidados e atendimentos que prestam;
- O compartilhamento dos dados permitirá diagnósticos e tratamentos mais proativos, assertivos e efetivos, melhorando o atendimento e reduzindo custos com repetições, internações e tratamentos invasivos;
- Medição precisa em relação ao uso, produtividade e desempenho dos seus recursos materiais e humanos.
- Suporte para aplicações de Inteligência artificial e aprendizado de máquinas, convergentes as Análises Preditivas e ao uso em Telemedicina com impacto direto na qualidade e custos de atendimento.

Na perspectiva dos governos municipais, estaduais e federal, os benefícios potenciais seriam os seguintes:

- Ações e serviços de bem-estar e saúde melhores, mais eficientes e com mais qualidade no atendimento individual, mas também em ações preventivas, que afetam a sociedade por políticas públicas e alocações de recursos de forma mais inteligente, eficiente e transparente;
- Dispor de dados para análise e percepção de focos de doenças, com medidas proativas de controle e combate no local, no grupo de risco e momento corretos.
- Medição precisa em relação ao uso, produtividade e desempenho de recursos materiais e humanos, cruzando verbas disponibilizadas com a eficácia e efetividade de sua aplicação. Assim qualquer órgão independente da sociedade pode realizar avaliações dos gastos públicos dando transparência a gestão.

Dentro da perspectiva dos pesquisadores científicos os benefícios potenciais seriam o acesso a dados para pesquisas mais complexos e precisos, permitindo avaliações em grupos populacionais abrangentes, em mais regiões e com maior densidade populacional, além de contar com segmentações mais precisas desses grupos.

E por fim, dentro da ótica da indústria, os benefícios potenciais seriam dados que indiquem necessidades e tendências, que permitam um melhor direcionamento de recursos de pesquisa e desenvolvimento, produção e logística. Assim, percebe-se que o compartilhamento de dados de saúde e bem-estar em *blockchain* trará uma grande capacidade de transformação na sociedade em razão dos benefícios possíveis.

Este trabalho descreveu uma proposta de arquitetura para responder aspectos em aberto e estabelecer conceitos para o compartilhamento seguro dos dados de saúde e bem-estar. O desenvolvimento e implementação de protótipo MVP (*Minimum Viable Product*) partirá de estudos baseados em levantamento bibliográfico, considerando o estado atual e tendências do ecossistema de saúde no Brasil; as suas legislações e normas; as questões de segurança e privacidade destes dados; as tecnologias e padrões para coleta e compartilhamento de dados sobre *healthcare*; as plataformas *blockchain Ethereum* e *Hyperledger*, candidatas a serem adotadas; e características e limitações de outras tecnologias abertas, candidatas a uso para interface web, banco de dados, etc. Com isto pode ser desenvolvido um ambiente computacional em redes distribuídas e cadeias de blocos com segurança, alta disponibilidade, escalabilidade, resiliência e baixo custo.

Como trabalhos futuros podem ser apontados: O desenvolvimento de protótipo de plataforma IoT para *healthcare*; desenvolver estudos para análises dos dados e ações preventivas através de inteligência artificial e aprendizado de máquina; e por fim, realizar estudos para aplicação em telemedicina dos dados através de visualização de dados,

aderentes as Resoluções 1643/2002 e 2228/2019 do Conselho Federal de Medicina.

REFERÊNCIAS

[1] IBGE, "Censo Demográfico 2010: Características gerais da população, religião e pessoas com deficiência", IBGE - Coordenação de População e Indicadores Sociais. – Rio de Janeiro, Rio de Janeiro, Brasil, 2010. Disponível: https://biblioteca.ibge.gov.br/visualizacao/periodicos/94/cd_2010_religiao_deficiencia.pdf.

[2] C. P. Duarte, C. L. dos Santos, A. K. Gonçalves., "A concepção de pessoas de meia-idade sobre saúde, envelhecimento e atividade física como motivação para comportamentos ativos". Revista Brasileira da Ciência dos Esportes, Campinas, v. 23, n. 3, p. 35-48, maio 2002.

[3] A. A. Shrier, A. Chang, N. Diakun-thibault, L. Forni, F. Landa, J. Mayo, R. van Riezen. "Blockchain and Health IT Algorithms, Privacy, and Data". Office of the National Coordinator for Health Information Technology - U.S. Department of Health and Human Services, Aug 2016. Disponível: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf .

[4] S. Nakamoto. "Bitcoin: A peer-to-peer electronic Cash System**"** BitCoin Org, 2008 – Disponível em: https://bitcoin.org/bitcoin.pdf .

[5] V. Buterin, "Ethereum – A Next Generation Smart Contract and Decentralized Application Platform", Disponível em: https://github.com/ethereum/wiki/wiki/White-Paper.

[6] Ministério da Saúde – "PORTARIA Nº 2.073, DE 31 DE AGOSTO DE 2011 - (Padrões de interoperabilidade e informação em saúde para sistemas de informação - SUS e para os sistemas privados e do setor de saúde suplementar)" Disponível: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html.

[7] United States Department of Health and Human Services. "Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009". Disponível: https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf.

[8] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles. "A Blockchain Approach to Health Information Exchange Networks". Mayo Clinic. Disponível: https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf.

[9] O. Bodenreider, D. Nguyen, P. Chiang, P. Chuang, M. Madden, R. Winnenburg, R. McClure, S. Emrick, I. D'Souza**.** "The NLM Value Set Authority Center", U.S. National Library of Medicine 2013. Pages 1224 – 1224, DOI 10.3233/978-1-61499-289-9-1224 Volume 192: MEDINFO 2013 Disponível: http://ebooks.iospress.nl/publication/34440.

[10] A. Buldas, R. Laanoja, and A. Truu. "Security Proofs for the BLT Signature Scheme", GuardTime AS, Tallinn, Estonia. 2014. Disponível: https://eprint.iacr.org/2014/696.pdf.

[11] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman. "A Case Study for Blockchain in Healthcare: 'MedRed' prototype for electronic health records and medical research data". Disponível: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf.

[12] Ministério da Saúde – "Portaria nº 940, de 28 de abril de 2011- (Regulamenta o Sistema Cartão Nacional de Saúde – Sistema Cartão)" Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt0940_28_04_2011.html.

[13] United States Department of Health and Human Services. "Summary of The HIPPA Privacy Rule". Disponível: https://www.hhs.gov/hipaa/index.html.

[14] CGU – Controladoria Geral da União. "Privacidade e Proteção de Dados Pessoais". 2017 – Brasília – Disponível: http://www.cgu.gov.br/sobre/institucional/eventos/2017/5-anos-da-lei-de-acesso/arquivos/mesa-3-danilo-doneda.pdf.

[15] COMISSÃO EUROPEIA, "The General Data Protection Regulation", final version dated 27 April 2016. Disponível http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

[16] Presidência da República, Casa Civil - Lei 13708/18 de 14/08/2018**.** "Lei Geral de Proteção de Dados". Disponível: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

[17] S. King, S. Nadal. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake". Peercoin. Agosto de 2012. Disponível: https://peercoin.net/assets/paper/peercoin-paper.pdf.

[18] I. Bentov, C. Lee, M. Rosenfeld, A. Mizrahi. "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake". NetEcon 2014– Workshop on the Economics of Networks, Systems and Computation. Austin, TX, USA. – June 2014

[19] G. Zyskind, O. Nathan, A. Pentland. "Decentralizing Privacy: Using Blockchain to Protect Personal Data". 2015 IEEE CS Security and Privacy Workshops. DOI 10.1109/SPW.2015.27

[20] G. Zyskind, O. Nathan, A. Pentland**. "**Enigma: Decentralized Computation Platform with Guaranteed Privacy", Disponível: < https://enigma.co/enigma_full.pdf .

[21] Tomas Mikula, Rune Hylsberg Jacobsen. "Identity an access Management with Blockchain in Electronic Healthcare Records", 2018 21st Euromicro Conference on Digital System, Design. pp. 699-706.

[22] Shan Jiang, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, Jianfei, "BlocHIE: A Blockchain-based plataform for Healthcare Information Exchange". 2018 IEEE International Conference on Smart Computing, pp-49-56, DOI 10.1109/SMARTCOMP.2018.00073.

[23] Christian Esposito, Alfredo de Santis, Genny Tortora, Henry Chang, Kim-Kwang Raymond Choo – "Blockchain: a Panacea for Healthcare Cloud-based data Security and Privacy", IEEE Cloud Computing – January / February 2018. pp- 31-27 - Copublished by the IEEE CS and IEEE ComSoc, 2325-6095/18/$33.00 ©2018 IEEE.

[24] Sofia Alexaki, George Alexandris, Vasilis Katos, Nikolaos E. Petroulakis, Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions, 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD).

Paulo Sérgio Rangel Garcia, graduado em Matemática no Complexo Educacional FMU (1986), Mestrado em Tecnologias da Inteligência e Design Digital pela Pontifícia Universidade Católica de São Paulo (2011). Doutorando em Engenharia da Informação na Universidade Federal do ABC. Atualmente é Professor na FMU, com interesse em Segurança da Informação, *Blockchain*, Sistemas Distribuídos, Sistemas para Bem-estar e Saúde, Comunicações sem fio, IoT, Compartilhamento e Visualização de dados.

João Henrique Kleinschmidt, graduado em Engenharia da Computação (2001), Mestrado em Ciência da Computação (2004) pela Pontifícia Universidade Católica do Paraná, e Doutorado em Engenharia Elétrica pela Universidade Estadual de Campinas (2008). Atualmente é Professor Associado na Universidade Federal do ABC, tendo interesse em Redes de Computadores, Sistemas Distribuídos e Segurança de Redes.