Blockchain e *Smart Contracts* aplicados no compartilhamento de dados pessoais de saúde e bem-estar

Paulo Sérgio Rangel Garcia e João Henrique Kleinschmidt
Universidade Federal do ABC
paulo.rangel@ufabc.edu.br e joao.kleinschmidt@ufabc.edu.br

Resumo: Para o compartilhamento de dados de saúde e bem-estar tornar-se realidade, precisam-se equacionar pontos como: infraestrutura de rede, segurança e interoperabilidade dos dados. Os modelos atuais têm estruturas centralizadas sensíveis a ataques, com estrutura e semântica de dados proprietárias limitando a interoperabilidade, além da necessidade de terceiro confiável para garantir a segurança. O uso de *blockchain* e *smart contracts*, oferece novas perspectivas através de rede distribuída, escalável e resiliente, com garantias de integridade por consenso, segurança no acesso através de contratos inteligentes, dispensando a confiança em terceiros. Neste trabalho discutiremos a tecnologia *blockchain* como viabilizadora de modelo para compartilhamento desses dados, vencendo os desafios de rede, segurança e interoperabilidade.

1. Introdução

Nas últimas décadas o envelhecimento da população apresentou forte crescimento, mantendo-se a tendência de aumento na expectativa de vida. Isso traz reflexos na faixa etária dos adultos jovens e de meia idade reforçando a importância em ter-se um estilo de vida saudável com atividades físicas, na busca da saúde do corpo e da mente, preparando-se para viver o amadurecimento de suas vidas de forma plena e ativa.

Este cenário indica que mais dados sobre bem-estar e saúde serão coletados em hospitais, clínicas, academias, etc., somando-se aos que são coletados em tempo real por dispositivos pessoais, que monitoram medidas biométricas em atividades físicas, aumentando o seu volume e importância. Também se nota que parte desses dados, em razão da dispersão, estruturas de dados e semântica divergentes, são pouco utilizados, recebendo pouca proteção.

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

Pode-se definir *Blockchain* como uma tecnologia que usa a descentralização de uma rede *peer-to-peer* como forma de segurança. São bases de dados distribuídas e compartilhadas, operando como um livro-razão público, compartilhado e universal, estabelecendo o consenso e confiança na comunicação entre duas partes, sem intermediários. A *blockchain* cresce à medida que novos blocos são adicionados com novos registros ou transações, de modo linear e cronológico. Assim, cada nodo da rede que tem a tarefa de validar e repassar transações, obtém uma cópia completa da *blockchain* com endereços e saldos, desde o primeiro até o último bloco incluído.

Desta forma, considerando as características de *Blockchain* e *Smart Contracts*, como: a adoção de rede distribuída *peer-to-peer* com algoritmo de consenso distribuído, sem um repositório central de dados, dispensando a figura central de um terceiro confiável; escalabilidade e resiliência testadas nas implementações de criptomoedas; suporte para contratos inteligentes e programáveis que estabelecem regras de relacionamento, direitos e obrigações entre as partes e por fim, API padrão de código aberto, amplamente difundida na comunidade de desenvolvedores, este trabalho propõe apresentar um modelo que vença o desafio identificado.

2. Algoritmos de consenso

Um dos problemas em processamento distribuído é a confiabilidade do sistema. Frequentemente necessita-se que os nodos concordem que algum dado é o correto. Assim exige-se um acordo entre certa quantidade de nodos, e mesmo que alguns não sejam confiáveis, o algoritmo definirá o que será adotado pela rede e que não mais será alterado.

Dentre os algoritmos de consenso destacam-se a Prova de Trabalho (do inglês *Proof of Work - PoW*) [1], a Prova de Participação (do inglês *Proof of Stake – PoS*) [3], a Prova de Importância (do inglês, *Proof of Importance – PoI*) [4] e a Prova do Tempo Decorrido (do inglês *Proof of Elapsed Time – PoET*)[1].

Em *Bitcoin*, com a PoW, o minerador ou qualquer nodo que queira inserir blocos na cadeia, a cada bloco, deverá antes resolver um complexo problema matemático, dispendendo tempo, energia e poder computacional. O nodo que primeiro o solucionar, será eleito o minerador que incluirá o novo bloco recebendo uma recompensa por isso.

3. Proposta

Pretende-se integrar os diversos atores do ecossistema de saúde e bem-estar em uma rede distribuída adotando a tecnologia *Blockchain* para garantir que os dados gravados tenham o consenso da rede e sejam: gravados cronológicamente, interoperáveis, seguros, sigilosos, e de alta disponibilidade. Para isso abordaremos a proposta sob os seguintes aspectos: Interoperabilidade, Segurança dos dados, inserção dos dados na cadeia (mineração), contratos inteligentes e integração com *middlewares*, conforme figura 1:

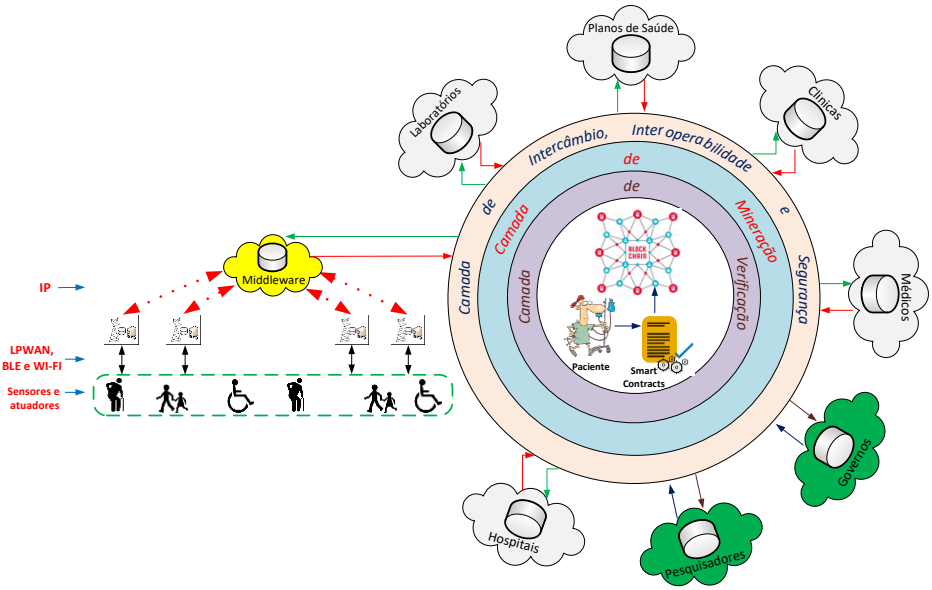

Figura 1 – Cenário proposto para uso de *Blockchain* na saúde e bem-estar

Como premissa, observar-se-á a Portaria do Ministério da Saúde nº 2073 de 31/08/2011, que define padrões de interoperabilidade para informações de Saúde no Brasil e as legislações sobre proteção de dados vigentes no País.

3.1. Interoperabilidade

Garantida através do algoritmo de consenso proposto por Peterson [2], chamado de Prova de Interoperabilidade (PdI), que ao contrário da PoW que consome energia e poder computacional sem agregar valor real ao processo, poder-se-ia então adotar uma prova de consenso que garanta a interoperabilidade do dado antes de ser inserido em um bloco. A adoção da PdI tem impacto no momento da eleição do nodo minerador que fará a inserção do bloco.

3.2. Quanto a Segurança dos dados

Os dados críticos e o *payload* da transação devem ser criptografados pelo nodo origem. Como a Prova de Interoperabilidade (PdI) será realizada por minerador eleito previamente, ele precisará ter acesso ao conteúdo plano da transação para validá-la, assim, além dele, apenas o nodo origem e o paciente deverão conhecer o conteúdo. Para isso, a transação será enviada ao minerador eleito criptografada com a sua chave pública, garantindo a privacidade do conteúdo. Após receber a transação e decodificá-la com sua chave privada, o minerador realizará a PdI, gerando uma chave única (simétrica) para cada transação, com a qual criptografará cada transação recebida. A chave única será criptografada com a chave pública do nodo 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. Assim garante-se que

[1] http://intelledger.github.io/introduction.html#proof-of-elapsed-time-poet

apenas o minerador, o nodo origem e o paciente terão acesso ao conteúdo quando já estiver gravado no bloco. Desta forma, mesmo que se comprometa a chave única, apenas está transação terá o seu conteúdo conhecido.

3.3. Inserção de dados na cadeia

Na PoW, é eleito como minerador o nodo que resolver primeiro o desafio matemático depois de ter formado o bloco a ser inserido. Na Prova de Interoperabilidade, a eleição do próximo minerador acontecerá por algoritmo que considerará o número aleatório enviado pelos nodos que participaram na formação do bloco atual, que determinará um resultado que corresponderá ao nodo ativo cujo número mais se aproximar desse resultado e que tenha uma certa quantidade de *tokens* que comprovem a sua participação na rede [2] [5], acontecendo esta eleição antes da formação do bloco. Combinando-se assim a Prova de Interoperabilidade e a Prova de Participação para determiná-lo.

Os nodos que tiverem transações a inserir na *blockchain* poderão enviá-lo direto ao minerador eleito economizando banda, processamento e energia. Resumidamente, o processo de inserção de dados na cadeia dar-se-á em estágios como proposto por Peterson [2] e levarão um tempo certo para permitir que o processo de coleta de transações e formação do novo bloco (momento T0), seguido da validação do novo bloco pelos nodos participantes (momento T1), sua devolução, assinada pelos nodos participantes e apuração do próximo minerador (momento T2) e por fim, (momento T3) o envio do bloco formado para todos os nodos da rede informando qual nodo será o próximo minerador, para quem deverão ser enviadas as novas transações. Assim, do início do momento T1 até o final do momento T3, todos os nodos devem aguardar a definição do minerador para enviar suas novas transações.

3.4. Contratos Inteligentes

A identificação do usuário na *blockchain* é a sua chave pública, o que se leva a considerar os endereços associados a *wallet*, da mesma forma que nas operações em criptomoedas, porém sem garantir um identificador universal, pois o paciente poderá ter mais de uma identificação na rede o que em relação as práticas atuais representa uma quebra de paradigma, pois a entidade deixa de atribuir o "endereço" do seu usuário, passando essa atribuição ao usuário, que comunicaria a entidade sua identificação na contratação da cobertura dos serviços.

Sobre o uso de contratos inteligentes, deverão garantir que a autorização seja codificada e executável, p.e., um paciente pode desejar que um médico acesse exames laboratoriais específicos ou a partir de uma determinada data. Como os contratos são inseridos como transações na *blockchain*, garante-se sua validade e auditoria.

3.5. Integração com *Middlewares*

A Internet da Coisas tem um forte poder de transformação na sociedade, onde pessoas e objetos passam a portar sensores e atuadores que comunicam-se enviando medições biométricas e ambientais, de localização e de estado, chegando a tomar decisões sem a intervenção humana.

Tais dispositivos geram uma quantidade significativa de dados de saúde e bem-estar, podendo medir, p.e., o batimento cardíaco, a qualidade do sono, a pressão sanguínea, a temperatura do ambiente, a unidade do ar, as distâncias percorridas e até perceber a queda de um paciente. Tais informações inseridas na *blockchain* podem gerar ações mais rápidas e proativas, melhorando a qualidade de vida dos usuários e reduzindo custos de tratamentos de saúde, antecipando ações que podem reduzir ocorrências de internações e/ou tratamentos invasivos.

4. Conclusão

Acredita-se que o modelo proposto utilizando-se *Blockchain* responda as questões em aberto e permita que os dados de saúde e bem-estar sejam interoperáveis, seguros, sigilosos, e disponíveis em rede única de alta disponibilidade, transformando-os em informação e conhecimento compartilhados, beneficiando o indivíduo e a sociedade.

5. Referências

[1] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic Cash System", BitCoin Org, 2008 - Disponível em: < https://bitcoin.org/bitcoin.pdf > Acesso em 10/08/2017

[2] Kevin Peterson, *et al*. "A Blockchain Approach to Health Information Exchange Networks". Mayo Clinic. Disponível em: < https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf> Acesso em 19/07/2017.

[3] KING, S.; NADAL, S. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake**"**. Peercoin. August 2012. Disponível em: < https://peercoin.net/assets/paper/peercoin-paper.pdf > Acesso em 20/09/2017.

[4] BENTOV, I.; et al. "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

[5] EKBLAM, A, *et al*. "A Case Study for Blockchain in Healthcare: "MedRed" prototype for electronic health records and medical research data". Disponível em: <https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf> Acesso em 19/07/2017.