Revista Brasileira de Computação Aplicada, Abril, 2020

DOI: 10.5335/rbca.v12i1.10752
Vol. 12, Nº 1, pp. 134–144
Homepage: seer.upf.br/index.php/rbca/index

ISSN 2176-6649

RELATO DE EXPERIÊNCIA

Modelo de negócio para saúde colaborativa usando *smart contracts*: caso TokenHealth

Health care business model using smart contracts: TokenHealth case

Vinicius Branco[1,2], Bruno Lippert[1,2], Roben Castagna Lunardi[1,3], Henry C. Nunes[1], Charles V. Neu[1,4], Avelino F. Zorzo[1], Diego Pirolla[5], Reider A. Bernucio[5], Sérgio Spacov[5]

[1]PUCRS, [2]DBServer, [3]IFRS, [4]UNISC, [5]TokenHealth

*{vinicius.branco,bruno.lippert,roben.lunardi,henry.nunes}@edu.pucrs.br; charlesneu@gmail.com; avelino.zorzo@pucrs.br

Recebido: 24/03/2020. **Revisado:** 02/04/2020. **Aceito:** 14/04/2020.

Resumo

Após a introdução do Bitcoin, a tecnologia de *blockchain* evoluiu como uma solução para fornecer integridade, não repúdio e disponibilidade de dados para diferentes sistemas. Cenários sensíveis a dados, como *Health Care*, também podem se beneficiar dessas propriedades da *blockchain*. Assim, diferentes propostas, tanto da Academia quanto da Indústria, foram implantadas para permitir a adoção de *blockchain* em aplicativos de assistência médica. No entanto, existem poucas discussões sobre métodos de incentivo para ajudar a motivar novos usuários a adotar sistemas de saúde. Além disso, pouco se discute sobre o desempenho para executar códigos em *blockchains* públicos e privados. Para resolver esses problemas, este trabalho apresenta uma avaliação do TokenHealth, um aplicativo para monitoramento colaborativo de práticas de saúde com gamificação e incentivos baseados em *tokens*, em diferentes redes da Ethereum. A solução proposta é implementada por meio de *smart contracts* usando a linguagem Solidity e executada em máquinas virtuais da Ethereum (EVM). Avaliamos o desempenho da rede de teste Ropsten e de uma instância privada da Ethereum. Os resultados preliminares mostram que a execução de *smart contracts* leva menos de um minuto para um ciclo completo de diferentes *smart contracts*. Além disso, apresentamos uma discussão sobre os custos do uso de uma instância privada e da rede principal pública do Ethereum.

Palavras-Chave: Blockchain, Contratos Inteligentes, Ethereum, Saúde

Abstract

After the introduction of Bitcoin, blockchain technology evolved as a solution to provide data integrity, non-repudiation, and availability for different systems. Especially data-sensitive scenarios, such as Health Care, can also benefit from these blockchain properties. Thus, different proposals, both from Academia and Industry, were deployed to allow the adoption of blockchain in Health Care applications. However, there are few discussions about incentive methods to help to motivate new users to adopt health-care systems. Also, little is discussed about performance to execute codes in private and public blockchains. In order to tackle these issues, this work presents an evaluation of TokenHealth, an application for collaborative health practice monitoring with gamification and token-based incentives, on different Ethereum networks. The proposed solution is implemented through *smart contracts* using the Solidity language and executed using Ethereum Virtual Machine (EVM). We evaluated the performance of both in the Ropsten test network and in a private Ethereum instance. The preliminary results show that the execution of *smart contracts* takes less than a minute for a full cycle of different *smart contracts*. Additionally, we present a discussion about costs for using a private instance and the public Ethereum network.

Keywords: Blockchain, *smart contracts*, Ethereum, Health Care

1 Introdução

[1] O conceito de *Blockchain* foi inicialmente introduzido para manter registro das transações da criptomoeda *Bitcoin* (Nakamoto, 2008). Contudo, atualmente, a *Blockchain* passou a ser utilizada na solução de uma série de diferentes problemas, tais como, serviço de DNS (Chang and Svetinovic, 2016), armazenamento e execução de trechos de código (Ethereum, 2017), controle de transações (Min et al., 2016), voto eletrônico (Moura and Gomes, 2017), controle de direitos autorais (Kishigami et al., 2015), registro de dados de dispositivos de internet das coisas (Lunardi et al., 2019) e cidades inteligentes (Michelin et al., 2018). Muitas destas diferentes aplicações são originadas graças as características de resiliência (devido ao caráter descentralizado da rede), não-repúdio (através do uso de assinatura digitais nas transações) e também pela imutabilidade dos dados (Zorzo et al., 2018). Portanto, *blockchain* provê confiabilidade nos dados que por ela são mantidos. Ainda, a escolha de qual blockchain e qual configuração a ser adotada é um tema complexo. Por exemplo, dependendo do cenário pode-se optar por *blockchains* privadas (mantidas por uma determinada entidade), consórcio (mantidas por um conjunto específico de entidades) ou pública (mantida por nós independentes) (Dedeoglu et al., 2020).

Especialmente no contexto de dados sobre a saúde, alguns estudos sugerem a aplicação de *blockchains* para garantir a integridade e disponibilidade dos dados (Azaria et al., 2016, Mettler, 2016, Guo et al., 2018). Dentre alguns problemas, podem ser citados dados que muitas vezes não são registrados corretamente, ou que podem estar desatualizados, e até, em muitos casos, não ficam sobre a posse dos pacientes (Azaria et al., 2016). Ainda, a falta de interoperabilidade de sistemas pode levar a registros duplicados e a realização desnecessária de novos exames médicos (Azaria et al., 2016). Além disso, a falta de mecanismos de controle de acesso aos dados pode comprometer o negócio de empresas do ramo de saúde (Mettler, 2016). Devido a natureza dos dados, e especialmente após a Lei Geral de Proteção de Dados (Brasil, 2018) ter sido aprovada no Brasil, a privacidade dos dados dos usuários passa a ter ainda mais impacto no negócio das empresas do setor de saúde (Guo et al., 2018).

Apesar das pesquisas na área de *blockchain* proporem soluções na área da saúde para armazenamento de dados digitalizados (Mertz, 2018), controle de acesso aos dados (Rifi et al., 2017) e compartilhamento de dados (Xia et al., 2017), pouco se discutiu sobre soluções com métodos de incentivos para usuários. Métodos de incentivo, seja através de bonificação ou de gamificação, vem atraindo muita atenção e sendo adotados em diversos sistemas que utilizam *blockchain* (Parizi and Dehghantanha, 2018). Isto ocorre devido a capacidade da execução de código de forma distribuída através do uso de *smart contracts*, também conhecidos como contratos inteligentes (Zyskind et al., 2015).

Desta forma, este trabalho tem como objetivo apresentar o projeto TokenHealth, um sistema de saúde colaborativo com métodos de incentivo utilizando *blockchain* e *smart contacts*. Consequentemente, o sistema busca garantir os aspectos de integridade, resiliência e disponibilidade, além de apresentar métodos de incentivos para a adesão dos usuários. Ainda, tem-se como objetivo a utilização de *smart contracts*, para garantir que as regras de negócio fiquem disponíveis de forma transparente, se mantenham íntegras e estejam protegidas contra usuários maliciosos. Para avaliar o desempenho em diferentes cenários, optou-se por avaliar a proposta tanto em uma rede de testes pública (Ropsten), quanto em uma instância privada da Ethereum (Ethereum, 2017). Em ambos os casos, utilizou-se contratos e nós de rede com base na Ethereum, uma das mais populares *blockchains* com suporte a *smart contracts*.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta e relaciona alguns trabalhos com a solução apresentada. A Seção 3 apresenta a solução conceitual do sistema, relatando o seu funcionamento, detalhes de como os *smart contracts* são utilizados no projeto, bem como relata as tecnologias utilizadas, principais pontos sobre a implementação e as limitações da solução. A Seção 4 apresenta os resultados preliminares obtidos. Por fim, a Seção 5 apresenta as considerações finais e trabalhos futuros.

2 Referencial Teórico

Com o sucesso da Bitcoin, outras *blockchains* começaram a surgir com propostas diferentes e novas tecnologias. A Ethereum, assim como outras *blockchains* que possuem uma criptomoeda (como o Bitcoin e o Litecoin) associada, utiliza o *Proof-of-Work* (PoW) como algoritmo de consenso (Tschorsch and Scheuermann, 2016). O algoritmo de consenso é um mecanismo utilizado para garantir que a adição de dados segue uma lógica de negócio pré-combinada. Isso se faz necessário pela *blockchain* funcionar em uma rede descentralizada *peer-to-peer* (p2p) onde os nodos participantes não são confiáveis, pois podem agir de forma maliciosa. O algoritmo de consenso garante que os dados gerados por qualquer nodo nesse ambiente não-confiável são dados confiáveis. A natureza dos dados gerados e da lógica de negócio funcionam de acordo com a solução de *blockchain* utilizada. Uma das possibilidades de solução para representação de lógicas de negócio em blockchain é através da utilização de *smart contracts* (Dedeoglu et al., 2020).

Na *blockchain* esses *smart contracts* possuem diferentes modelos de utilização. Por exemplo, o modelo utilizado pela Hyperledger Fabric (Cachin, 2016) e o modelo utilizado pela Ethereum. Apesar de funcionarem de forma diferente resultam na possibilidade de executar programas diretamente na blockchain. Estes programas são processados pela rede da *blockchain*, dando flexibilidade para uma *blockchain* poder processar qualquer aplicação implementada em *smart contract*. Como são processados na *blockchain*, são decentralizados, o

[1] Este trabalho é uma versão estendida do Melhor Artigo da Escola Regional de Redes de Computadores (ERRC 2019) (Branco et al., 2019).

que pode trazer benefícios para aplicações especificas. Outras vantagens são a imutabilidade das informações geradas, transparência do funcionamento e a auditabilidade das computações feitas.

No caso da Ethereum, cada nodo possui uma máquina virtual, chamada de Ethereum Virtual Machine (EVM), que pode processar *bytecodes* representando *smart contracts*. Os usuários podem fazer solicitações especiais para a rede, com chamadas para esses *smart contracts*, permitindo que eles alterem seu estado ou solicitar informações sobre o estado atual dos *smart contracts*. Os nodos irão processar essas solicitações com o *bytecode* do *smart contract* em questão na sua EVM e o estado resultante do *smart contract* será armazenado na *blockchain* (Ethereum, 2017).

Em um trabalho realizado por Rouhani and Deters (2019), são discutidas questões de segurança e desempenho da execução de *smart contracts*. Por exemplo, são mencionados diferentes trabalhos que tentam medir o desempenho de *smart contracts*. São citadas algumas métricas, como o número de transações por segundo, o tempo para a execução de contratos e o tempo de atualização de estado do bloco. Para fins de medição, neste trabalho, será adotado o tempo médio para a realização de cada contrato.

Para resolver o problema de concentração da mineração em um número limitado de nós, (Kano and Nakajima, 2017) propõe um novo incentivo ao uso baseado na gamificação. A proposta se destaca por utilizar uma forma diferente de incentivo aos métodos tradicionais (usados em criptomoedas) presentes nos principais algoritmos de mineração. Os autores apresentam experimentos que mostram a viabilidade de adotar o incentivo alternativo, bem como discutem os impactos positivos dos fatores psicológicos proporcionados pelos métodos de gamificação.

Parizi and Dehghantanha (2018) também discutem o processo de gamificação em *blockchains*. Os autores sugerem que estratégias de gamificação tendem a ser bastante utilizadas em abordagens centradas em humanos, especialmente no mundo online, tanto na indústria, negócios e academia. Os autores também identificaram e discutiram os principais problemas relacionados à humanos em sistemas baseados em *blockchain* e propuseram um modelo com gamificação.

Outro trabalho que discute benefícios em sistemas baseados em *blockchain* é apresentado por Chen et al. (2018). Seu método é construído como um novo tipo de aliança de pontos de bônus descentralizados, com base nas principais tecnologias da *blockchain*, como mecanismo de consenso e *smart contracts* e a " aliança *blockchain*". Esta proposta aproveita os recursos técnicos de descentralização, confiança-consenso, rede distribuída, manutenção coletiva e pesquisa avançada sobre o modelo de negócios da BonusPoints Alliance baseado em *blockchain*. Este modelo é aplicado de forma a projetar um sistema que possa ser usado para resolver deficiências atuais nos programas de bonificação tradicionais, tais como o alto custo de desenvolvimento do sistema e a dificuldade de troca e de circulação de pontos de bônus.

Um sistema de repúdio baseado em *blockchain* é proposto por Dennis and Owen (2015). Os autores discutem os sistemas de reputação atuais, as vulnerabilidades de segurança atuais e como as novas tecnologias baseadas em *blockchain* são usadas atualmente. Seu objetivo é propôr um novo sistema de reputação baseado em tecnologias *blockchain* para resolver problemas que, segundo os autores, ainda não foram resolvidos nos sistemas de reputação. Os resultados são apresentados e discutidos com base em simulações. O desempenho é avaliado e as limitações da solução proposta são indicadas e explicadas. Por fim, os autores também apresentam sugestões para resolver limitações atuais e sugestões para trabalhos futuros.

Com foco no controle de acesso de dados de saúde, Guo et al. (2019) propõe uma solução híbrida para armazenar e disponibilizar acesso aos dados de saúde. O trabalho propõe o uso de dados de dispositivos de internet das coisas (que armazenam informações de saúde) juntamente com dados hospitalares. Ainda que a proposta traga uma arquitetura interessante, os autores não tratam como interligar e aproximar os usuários das organizações de saúde.

Shahnaz et al. (2019) propuseram um sistema baseado em smart contracts para registro de informações de saúde. Ainda, o trabalho em questão discute um sistema de camadas de acesso aos dados, garantindo que determinados dados sejam mantidos privados ou tenho acesso restrito. Porém, os autores não discutem métodos de incentivo para as organizações e usuários do sistema.

Apesar de diferentes trabalhos apresentarem soluções para bonificação e gamificação dos usuários, poucas solução propões métodos de incentivo para a saúde colaborativa. Portanto, nas próximas seções deste artigo iremos descrever e avaliar o sistema proposto.

3 Prova de Conceito: TokenHealth

TokenHealth[2] é um sistema que visa promover a saúde através de uma ferramenta colaborativa, com métodos de incetivo (*tokens*) e gamificação (sistema de reputação). Para validar a ideia, optou-se por implementar uma prova de conceito de um fluxo de vacinação. Esta prova de conceito visa cobrir todo o ciclo de vacinação, desde a solicitação, aplicação lembrete de reaplicação, e gamificação/incentivos.

Ainda, esta prova de conceito tem como pilares a integridade, disponibilidade, e transparência, funcionalidades estas que podem ser obtidas através da adoção de *blockchain*. Adicionalmente, as regras de negócio utilizam *smart contracts* desenvolvidos usando a linguagem *Solidity*. Desta forma, propôs-se um modelo genérico de funcionamento, onde usuários podem manter seus registros de vacina atualizados e receber bonificações ao cuidar da saúde. A Fig. 1 apresenta uma visão geral do funcionamento e do fluxo dos principais componentes do sistema e a interação com os atores envolvidos.

[2]Direitos Autorais e uso do modelo de negócio explícito neste artigo são de propriedade dos seus idealizadores: Diego Pirolla, Reider Arnaud Bernucio e Sérgio Spacov.

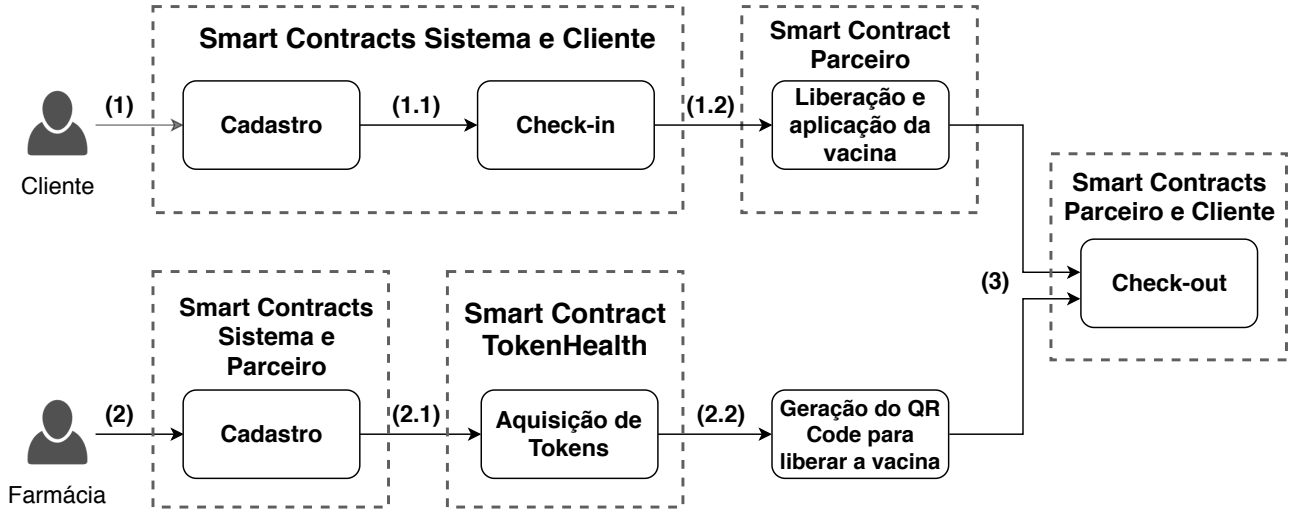

Figura 1: Fluxo do sistema de vacinação (Branco et al., 2019)

O fluxo do sistema TokenHealth depende de dois atores: *(i)* o cliente que necessita a vacina (para si ou seu dependente) e *(ii)* um local de vacinação (na Fig. 1 é utilizada uma farmácia como exemplo de local de vacinação). A proposta deste fluxo é conectar clientes e empresas de vacinação, estimulando que o cliente mantenha sua grade de vacinas atualizada. Além disso, os clientes podem ser bonificados com *tokens*, os quais podem ser utilizados para receber descontos em outras compras, assim, fidelizando o cliente às empresas que utilizam o sistema TokenHealth. Para isto, utilizou-se a tecnologia *blockchain*, mais especificamente da *blockchain* Ethereum, que permite criar transações que persistem dados seguindo regras de negócio, além de permitir enviar *tokens*, uma forma de "criptomoeda", que permite gerar valor de troca.

O fluxo é iniciado com o cadastro, tanto do cliente quanto da empresa, (fluxo 1 e 2, respectivamente na Fig. 1). O cliente, utilizando os *smart contracts* "Sistema e Cliente", informa seus dados pessoais, cadastra seus dependentes e as vacinas que já foram recebidas por cada um. Em um outro fluxo, a farmácia informa seus dados, endereço e registra as vacinas que possui disponíveis nos *smart contracts* "Sistema e Parceiro". Com os cadastros finalizados, a farmácia pode realizar a aquisição dos *tokens* que serão transferidos aos clientes como bonificação, conforme ilustrado no fluxo 2.1 na Fig. 1. O cliente pode, por exemplo, verificar quais vacinas devem ser aplicadas, selecionar um parceiro que tem a vacina desejada disponível e realizar o *check-in* no mesmo, podendo escolher entre pagar o valor integral da vacina e receber *tokens*, ou usar seus *tokens* para receber um desconto no valor da vacina, conforme ilustrado no fluxo 1.1 na Fig. 1.

Após o *check-in* ser realizado, o cliente deve deslocar-se até a farmácia, onde um atendente poderá visualizar o *check-in* no sistema "Parceiro TokenHealth"e gerar um QR Code único para o fluxo atual, para que o cliente, no aplicativo TokenHealth, faça a leitura e confirme a liberação da vacina para aplicação. Estas etapas são ilustradas nos fluxos 2.2 e 1.2 na Fig. 1. Assim que a vacina for aplicada, o atendente da farmácia poderá fazer este registro no sistema "Parceiro TokenHealth"através do processo de *check-out*, que é ilustrado no fluxo 3 na Fig. 1. O processo de *check-out* é concluído após ambas as partes confirmarem a realização completa do fluxo. Caso o cliente tenha optado pelo pagamento do valor integral da vacina, o parceiro realiza a confirmação para que o sistema envie automaticamente os *tokens* para o cliente, realizando o processo de bonificação. Entretanto, caso tenha optado por usar seus *tokens* como forma de pagamento e receber um desconto, após a confirmação do parceiro, o cliente deverá, novamente fazer a leitura de um QR Code para a realização do *check-out* a transferência de *tokens* do cliente para o parceiro.

4 Implementação

Para desenvolvimento da solução foi escolhido um conjunto de tecnologias que pode ser dividido em dois grupos: (*i*) tecnologias utilizadas para o desenvolvimento da aplicação, como linguagens de programação, bibliotecas e *Application Programming Interface* APIs; e (*ii*) tecnologias utilizadas como infraestrutura.

Para o desenvolvimento da interface *web* da aplicação da empresa parceira, utilizou-se JavaScript. Esta linguagem foi escolhida por estar consolidada no ambiente *web* e por possuir integração com as bibliotecas escolhidas. Todavia, para o aplicativo móvel do cliente foi utilizado o *framework Flutter*, devido a possibilidade de gerar executáveis tanto para *Android* quanto para *iOS* com o mesmo código fonte. Adicionalmente, a linguagem Solidity foi escolhida para o desenvolvimento de *smart contracts*, linguagem esta utilizada por padrão pela *blockchain* Ethereum. Ainda, utilizou-se as bibliotecas *React.js*, para criação da interface *web* e as bibliotecas *Web3DART Web3.js* para realizar a comunicação com a *blockchain*.

4.1 Arquitetura da solução

A solução desenvolvida consiste em três sistemas intendentes e uma instância da *blockchain* Ethereum. Os sistemas desenvolvidos consistem em um aplicativo *mobile* para o cliente que receberá a vacina, um sistema *web* para o parceiro que oferecerá a vacina e um sistema *web* para o administrador TokenHealth gerenciar os *tokens* da solução e ter informações das vacinações, como demonstrado nas Figs. 2 e 3.

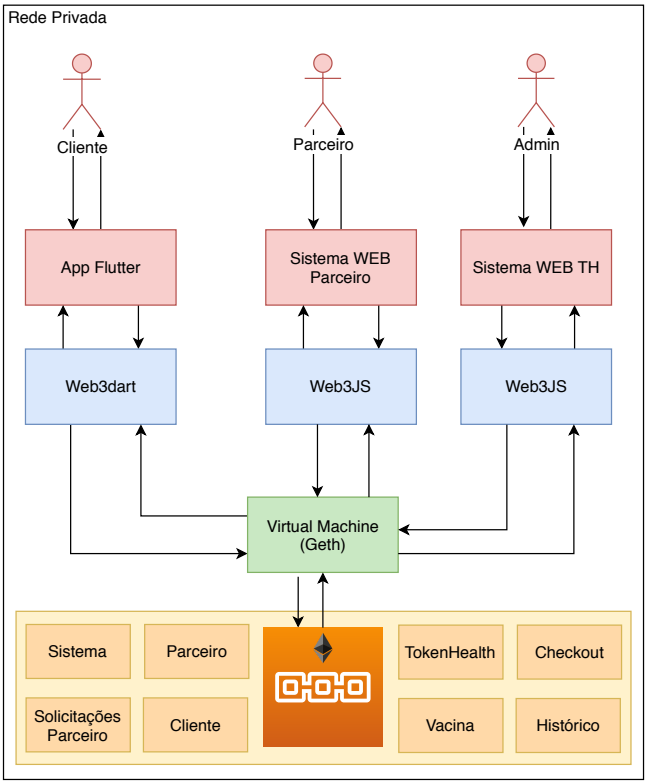

Figura 2: Arquitetura da solução - instância privada

Ainda, pode-se visualizar as duas redes da Ethereum utilizadas na solução, a privada (Fig. 2) e pública (Fig. 3) (tanto a rede principal da Ethereum, quanto a rede Ropsten são públicas). Para realizar o acesso às redes foi utilizado o conjunto de bibliotecas Web3 que provê uma *API* para comunicação com a rede. Na instância privada estas bibliotecas foram utilizadas para acessar o Geth (aplicação para criação de um nodo Ethereum, permitindo a criação de uma rede privada). Para realizar a comunicação com a rede pública da Ethereum foi utilizado o Infura (Infura, 2020).

4.2 Sistema do parceiro

O sistema *web* desenvolvido para o parceiro TH permite que o parceiro faça a compra de *tokens*, cadastre as vacinas oferecidas e realize o fluxo de vacinação. Para seu desenvolvimento utilizou-se da biblioteca *React.js*, que possibilita uma fácil integração com a rede *blockchain* através da biblioteca *Web3.js*. Um dos principais motivos para a escolha do *React.js* para desenvolver o *front-end* da aplicação é devido à biblioteca oferecer responsividade para diferentes tipos de aparelhos, como *smartphones* e *tablets*. A Fig. 4 ilustra a tela deste sistema.

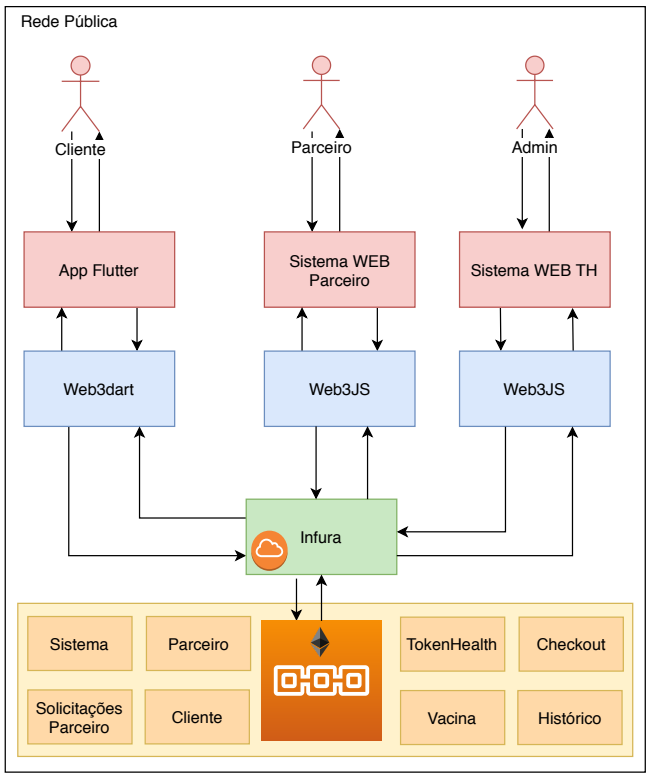

Figura 3: Arquitetura da solução - instância pública

4.3 Sistema da TokenHealth

O sistema TokenHealth, cuja tela principal é ilustrada na Fig. 5, é responsável pela manutenção da aplicação, assim como o gerenciamento de usuários e a venda dos *tokens*. Assim como o sistema do parceiro TH, também foi desenvolvido com *React.js* usando a biblioteca *Web3.js* para conexão com a *blockchain*.

4.4 Aplicativo do cliente

O sistema do cliente é um aplicativo móvel que provê todas as funcionalidades da plataforma para o cliente final, tais como o agendamento de vacinação, onde se inicia todo o fluxo de gamificação da plataforma. Pelo aplicativo móvel também é possível realizar a assinatura do contrato, garantindo que o cliente que está sendo vacinado é realmente o que marcou a consulta, assegurando que a gamificação vai ocorrer corretamente. Na Fig. 6 é apresentada a tela de checkin com o preço diferenciado com e sem uso de TH. Para fechamento do fluxo de vacinação, onde ocorre a gamificação de tokens, é confirmada a vacinação pelo cliente. Além

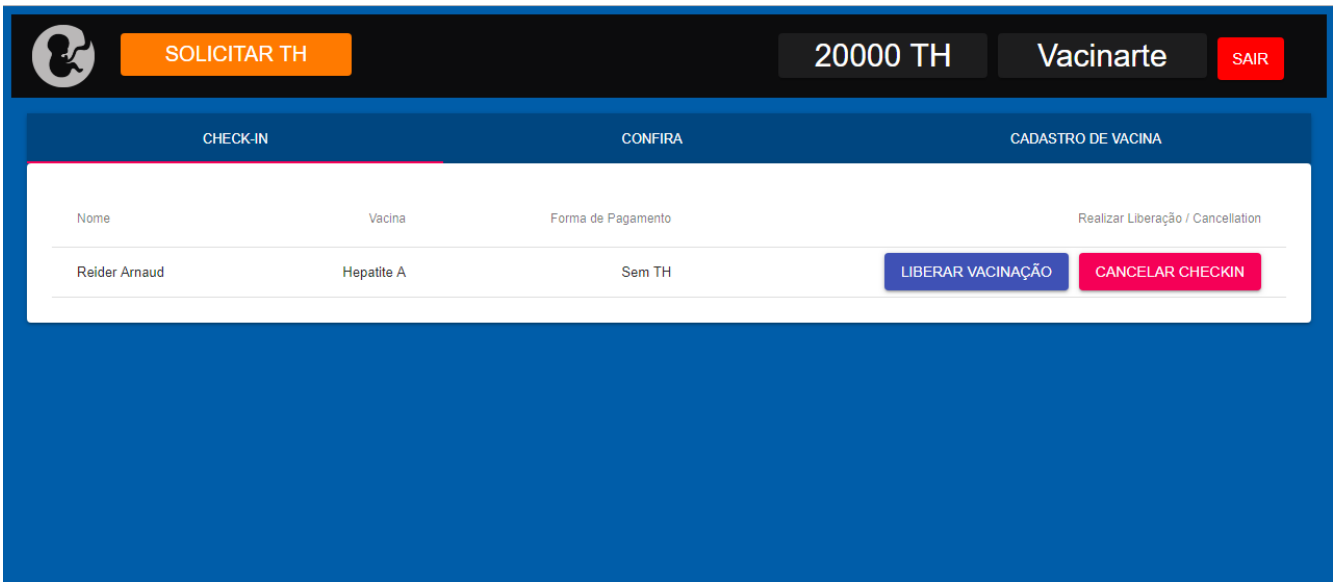

Figura 4: Sistema do parceiro TH

Figura 5: Sistema de administração TokenHealth

disso, o aplicativo disponibiliza informações sobre as quantidades de tokens da conta, locais de vacinação (geograficamente mais próximos) para facilitar o agendamento, gerenciamento de todas as contas dependentes e controle de vacinas efetuadas e agendadas.

Para o desenvolvimento da solução foi utilizada a linguagem Dart com o framework Flutter, que permite o desenvolvimento multiplataforma, também disponibilizando a biblioteca Web3Dart que facilita o acesso à rede da Ethereum, conforme demonstrado anteriormente nas Figs. 2 e 3.

5 Avaliação

Para avaliar a solução, utilizou-se a *Ropsten Test Net*, uma *blockchain* de teste mantida pela Ethereum. Este ambiente permite testar com facilidade os *smart contracts*, em um ambiente emulado, o qual possui características similares às encontradas na rede principal da Ethereum. Uma das principais vantagens de utilizar a Ropsten está no fato de não ser necessário o uso da criptomoeda Ether da *blockchain* principal da Ethereum para realizar transações. Na *Ropsten* são utilizadas criptomoedas "simbólicas"para viabilizar o teste de aplicações, e não é preciso manter uma infraestrutura para manter a *blockchain*, pois é mantida pelos próprios mi-

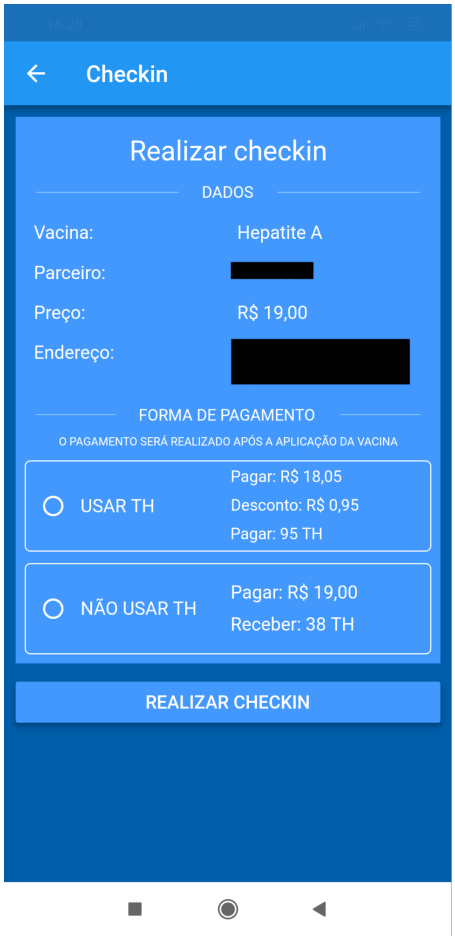

Figura 6: Tela de checkin do aplicativo do cliente

neiros da rede. Ainda, realizou-se experimentos com uma instância privada da Ethereum em um ambiente de nuvem (usando máquinas virtuais da Google Cloud Platform (Google Inc., 2019)). É importante ressaltar que não foi realiza avaliação de desempenho na rede principal da Ethereum devido aos custos financeiros envolvidos.

Uma vantagem em utilizar instâncias privadas está no fato de ser possível definir previamente a dificuldade de mineração do bloco gênesis. Esse recurso pode auxiliar a inicialização da *blockchain* com uma dificuldade que tenha uma Prova de Trabalho (Proof-of-Work - PoW) ajustada à infraestrutura que será usada para manter a *blockchain*. Desta forma, possibilita definir uma dificuldade que permite que a avaliação do tempo para criar novos blocos com uma taxa de transferência mais alta do que na rede pública Ethereum principal.

A Tabela 1 apresenta uma discussão qualitativa sobre o uso das diferentes redes da Ethereum para instanciar a solução proposta. Em nossa avaliação, as instâncias privada e Ropsten tiveram um tempo de de confirmação da inserção do *smart contract* menor que 1 minuto. Consequentemente, o comportamento em ambas foi semelhante. No entanto, na rede pública principal da Ethereum, o tempo de confirmação de inserção de transação é sempre superior a 1 minuto (usualmente acima dos 5 minutos). Isso ocorre devido à alta dificuldade presente na rede principal da Ethereum pública, devido ao aumento dinâmico da dificuldade ao longo do tempo (principalmente devido ao alto poder computacional dos mineradores). No entanto, quando um aplicativo distribuído (dApp) usa uma instância privada do Ethereum, há um custo de infraestrutura associado que deve ser considerado. Por exemplo, para uma aplicação simples, 5 nós são suficientes para validar blocos produzidos. No entanto, para aplicações maiores, mais nós devem ser usados para garantir resiliência e desempenho na execução de contratos inteligentes. Como pode ser observado na tabela, apenas na rede privada da Ethereum é possível regular a dificuldade inicial de mineração. Desta forma, pode-se adequar a dificuldade do algoritmo de PoW para produzir novos blocos em menor tempo. Ainda, tanto na instância privada da Ethereum, quanto na rede de teste da Ropsten, é possível gerar e executar *smart contracts* sem a necessidade de compra ou mineração de Ethers, diferentemente da rede principal.

A Tabela 2 mostra os custos de execução de cada contrato inteligente, aprenstando uma visão geral dos custos de manutenção da solução proposta. Primeiramente, analisando a rede pública da Ethereum, analisou-se o custo em *gas* (taxa para execução de contratos). O custo mais elevado para a execução de um *smart contract* individual (conforme mostrado na Tabela 2) é o custo para criar um novo membro, correspondendo a um total de 0,002718 Ethers (ou 0,731142 dólares, usando a cotação média de 269 dólares por Ether, do dia 16/02/2020 (Coin Market Cap, 2020)). Um usuário completo custa pelo menos 0,003136 Ethers (soma da nova conta e custos de um novo membro). Embora essa função tenha o custo mais alto, ela ocorrerá apenas uma vez por usuário.

O custo total para a execução completa do ciclo completo de vacinação (*checkin*, confirmação e *checkout*) requer 0,000776 Ethers (ou aproximadamente 0,208744 dólares). Isso se justifica pelo pequeno tamanho e processamentos exigido pelos *smart contracts* usados no ciclo de vacinação.

Como contraponto, para execução em instância privada da Ethereum, pode-se utilizar serviços em nuvem com custos pré-definidos para a infraestrutura. Por exemplo, ao alocar 5 máquinas específicas para rodar nós Ethereum no Google Cloud Platform (Google Inc., 2019), o custo fixo mensal ficaria por volta dos 123,75 dólares (5 instâncias de 24,75 dólares). Vale destacar, que neste cálculo estão sendo considerados apenas os custos básicos da locação de máquinas virtuais e não estão sendo considerados os custos de manutenção e configuração do sistema.

Algumas observações podem ser feitas ao comparar os custos da rede principal do Ethereum público e de uma instância privada. Por exemplo, a rede principal da Ethereum pública não exige custo de manutenção e o custo de cada execução é baseado no número de ciclos. No entanto, o uso de uma instância privada pode permitir um número maior de transações com um custo fixo. Como comparação, a principal rede pública Ethereum pode executar mais de 1.000 ciclos completos

Tabela 1: Diferenças dos diferentes usos da *blockchain* Ethereum para uso por *dApps* (Branco et al., 2019)

	Ethereum (Principal)	**Ropsten (rede de testes)**	**Instância Privada**
Tempo de Mineração	>5 minutos	<1 minuto	<1 minuto
Dificuldade de Mineração	Alta	Média	Inicial Regulável
Custo Financeiro	Sim (Ethers)	Não	Sim (Infraestrutura)

de vacinação pelos mesmos US 123,75 dólares (considerando o valor de troca do Ether em 16 de Fevereiro de 2020 (Coin Market Cap, 2020)).

Considerando o objetivo do aplicativo desenvolvido, mil ciclos não são suficientes. Consequentemente, a rede principal da Ethereum tem um custo mais alto para executar os contratos inteligentes, considerando um sistema apenas para vacinação. Essa discussão deve ser explorada em uma avaliação futura, considerando outras entidades de assistência à saúde, como hospitais, seguro de saúde, academias e dentre outros.

Para a avaliação preliminar do desempenho dos *smart contracs* da solução, utilizou-se da rede testes Ropsten e de uma instância privada no Google Cloud (Google Inc., 2019) com 2 núcleos de processamento, 8GB de memória e 80GB de armazenamento. Os testes foram repetidos 10 vezes, sendo apresentados os resultados da mediana das execuções. Tanto na instância privada, quanto na rede de testes Ropsten, obtiveram-se bons resultados quanto ao desempenho, como pode ser observado na Fig. 7.

Podemos observar, na Fig. 7, que a execução de alguns *smart contracts* tem desempenho semelhante na instância privada e na Ropsten. Por exemplo, o contrato inteligente para criar uma Nova Conta executada em 27.744,5 milissegundos (mediana do tempo de execução) em uma instância privada e em 31.560,5 milissegundos na Ropsten, ou seja, uma diferença de cerca de 13%. No entanto, se considerarmos a execução de um *smart contract* com poucos requisitos de processamento (bytecode mais curto), a diferença é maior. Por exemplo, o contrato inteligente para adicionar um novo membro foi executado em 8.906 milissegundos na instância privada e em 69.533,5 milissegundos na Ropsten.

Além disso, é importante observar que o Ropsten tem um comportamento semelhante ao da rede principal do Ethereum público quanto a instabilidade da rede, *i.e.*, em alguns momentos a taxa de transferência pode ser afetada por problemas como resoluções de bifurcação da cadeia principal ou outros problemas. Para o ciclo completo de vacinação completo, ou seja, a soma do tempo gasto na execução dos *smart contracts* de *checkin*, confirmação de vacinação e *checkout*, foram necessários 44.273,5ms na instância privada e 69.899,5ms na rede de teste Ropsten.

Os resultados demonstram a viabilidade, considerando o desempenho, para executar os principais contratos inteligentes de um dApp para vacinação. No entanto, não foi possível comparar com a principal rede pública Ethereum devido aos custos financeiros da aquisição de Ethers.

6 Considerações Finais e Trabalhos Futuros

O cuidado com a saúde é sempre um tópico recorrente na sociedade, a cada dia surgem diversos avanços, técnicas novas e medicamentos, sendo assim é necessário criar meios de incentivar o cidadão a utilizá-los. Além disso, estão disponíveis uma diferentes de sistemas e aplicações para monitoramento de atividades de saúde e atividades de saúde. No entanto, é importante criar métodos para promover a adoção e uso pelos usuários finais, especialmente para uma abordagem colaborativa que possa ajudar a prevenir doenças e problemas de saúde. Desta forma, neste artigo foi apresentada uma solução para sistemas de economia colaborativa para a saúde utilizando *blockchain*, exemplificando a usabilidade desta tecnologia com o objetivo de melhorar a saúde e prevenção de doenças através da gamificação e fidelização.

Além disso, foram apresentados os *trade-offs* da utilização de *blockchain* em instâncias privadas ou em redes públicas de *blockchain*. Como demonstrado, os custos na rede pública da Ethereum são elevados quando o número de transações for alto. Porém, quando é escolhido utilizar instância privada, o custo de infraestrutura e pessoal devem ser levados em conta. Ainda, observou-se que o desempenho na rede de testes se aproximou com os valores obtidos na instância privada, porém não foram obtidos resultados com a rede pública da Ethereum.

Por fim, conclui-se que utilizar *blockchain* é uma alternativa para sistema de economia colaborativa para a saúde, pois torna o sistema seguro por prover a imutabilidade dos dados, garantia de que uma lógica de negócio deve ser seguida e possibilidade de gamificação ao concluir uma ação de saúde preventiva.

Pretende-se, como trabalhos futuros, expandir o sistema para abranger, além de vacinas, medicamentos, consultas médicas e outras práticas que levam a manutenção da saúde preventiva. Ainda, pretende-se ampliar os testes na rede pública da Ethereum. Por fim, pretende-se avaliar o uso de *smart contracts* em diferentes *blockchains*, em especial *blockchains* permissionadas e com diferentes algoritmos de consensos, em especial Hyperledger Fabric (Cachin, 2016) e SpeedyChain (Lunardi et al., 2018, Michelin et al., 2018, Lunardi et al., 2019, Nunes et al., 2020).

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal Nível Superior – Brasil (CAPES) – Código de Financiamento 001. Avelino

Tabela 2: Custos de execução de *smart contracts*

	Ethereum (Rede Principal)	Instância Privada
Criação de Conta	0.000418 Ethers (~US$0,112442)	-
Adição de Membro	0.002718 Ethers (~US$0,731142)	-
Checkin	0.000739 Ethers (~US$0,198791)	-
Confirmação da vacinação	0.000003 Ethers (~US$0,000807)	-
Checkout	0.000034 Ethers (~US$0,009146)	-
Ciclo completo de vacinação	0.000776 Ethers (~US$0.208744)	-
Custo Mensal de Infraestrutura	-	US$123,75

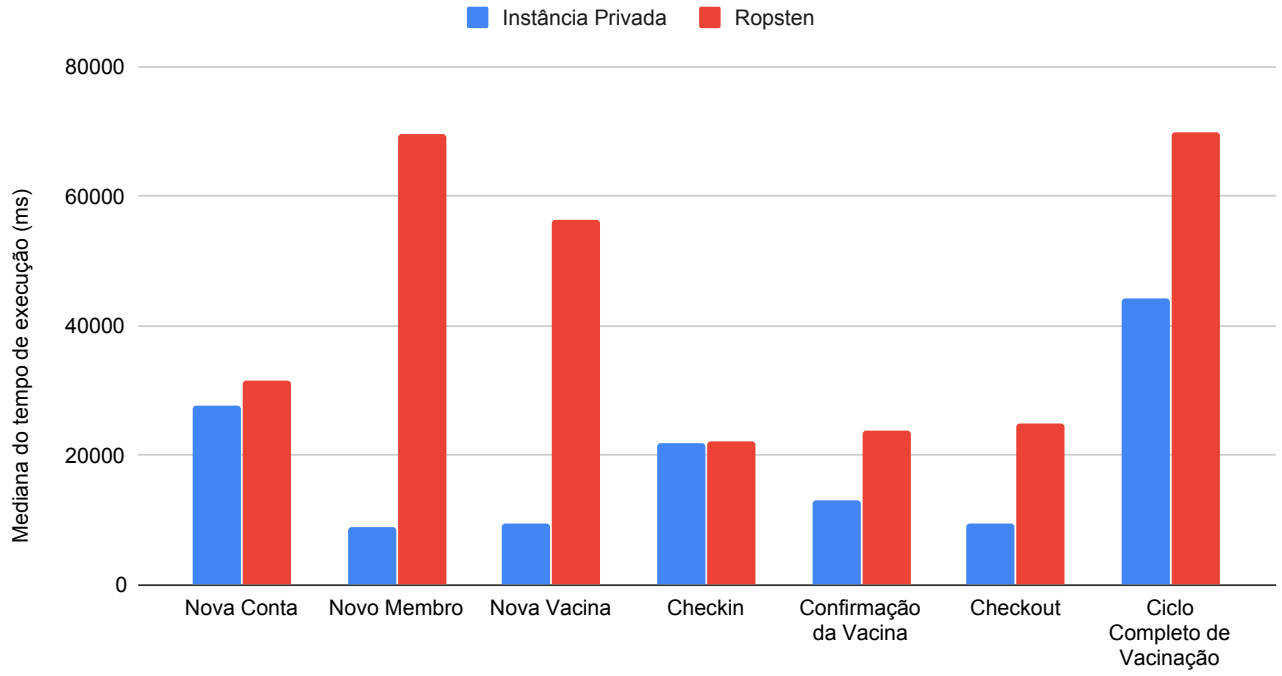

Figura 7: Desempenho para execução de *smart contracts* (Lunardi et al., 2019a)

F. Zorzo é apoiado pelo CNPq (315192/2018-6). Este trabalho foi apoiado pela INCT Ciências Forenses, através do Conselho Nacional de Desenvolvimento Científico e Tecnológico (Processo CNPq #465450/2014-8). Ainda, o trabalho recebeu apoio da HP Brasil usando incentivos da Lei da Informática (Lei n 8.248 de 1991), pelo IFRS e pela DB Server. Adicionalmente, o trabalho foi desenvolvido em conjunto com a TokenHealth.

Referências

Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management, *2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30. http://doi.org/10.1109/OBD.2016.11.

Branco, V., Lippert, B., Nunes, H., Lunardi, R. and Zorzo, A. (2019). Avaliação do uso de Smart Contracts para Sistema de Saúde Colaborativa, *17a Escola Regional de Redes de Computadores*, Alegrete-RS, Brasil. Disponível em http://errc.sbc.org.br/2019/papers/\branco2019avaliao.pdf.

Brasil (2018). Lei geral de proteção de dados (lgpd). Dísponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm.

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric, *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*.

Chang, T. H. and Svetinovic, D. (2016). Data analysis of digital currency networks: Namecoin case

study, *2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS)*, pp. 122–125. http://doi.org/10.1109/ICECCS.2016.023.

Chen, C., Sun, X., Lu, G., Kang, H. and Shen, Y. (2018). Bonus points alliance based on the blockchain, *14th International Conference on Semantics, Knowledge and Grids (SKG 2018)*, pp. 229–234. http://doi.org/10.1109/SKG.2018.00045.

Coin Market Cap (2020). Cryptocurrencies by market capitalization. Disponível em: https://coinmarketcap.com/.

Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R. C., Michelin, R. A., Zorzo, A. F. and Kanhere, S. S. (2020). Blockchain technologies for iot, *in* S. Kim and G. C. Deka (eds), *Advanced Applications of Blockchain Technology*, Springer Singapore, Singapore, pp. 55–89. https://doi.org/10.1007/978-981-13-8775-3_3.

Dennis, R. and Owen, G. (2015). Rep on the block: A next generation reputation system based on the blockchain, *10th International Conference for Internet Technology and Secured Transactions (ICITST 2015)*, pp. 131–138. http://doi.org/10.1109/ICITST.2015.7412073.

Ethereum (2017). A Next-Generation Smart Contract and Decentralized Application Platform. Disponível em: https://github.com/ethereum/wiki/wiki/White-Paper. Acessado em: 16-02-2020.

Google Inc. (2019). Google cloud platform. Disponível em: https://cloud.google.com/.

Guo, H., Li, W., Nejad, M. and Shen, C. (2019). Access control for electronic health records with hybrid blockchain-edge architecture, *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 44–51. http://doi.org/10.1109/Blockchain.2019.00015.

Guo, R., Shi, H., Zhao, Q. and Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, *IEEE Access* **6**: 11676–11686. http://doi.org/10.1109/ACCESS.2018.2801266.

Infura (2020). Infura documentation: Infura documentation. Disponível em: https://infura.io/docs.

Kano, Y. and Nakajima, T. (2017). An alternative approach to blockchain mining work for making blockchain technologies fit to ubiquitous and mobile computing environments, *10th International Conference on Mobile Computing and Ubiquitous Network (ICMU 2017)*, pp. 1–4. http://doi.org/10.23919/ICMU.2017.8330097.

Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A. and Akutsu, A. (2015). The blockchain-based digital content distribution system, *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*, pp. 187–190. http://doi.org/10.1109/BDCloud.2015.60.

Lunardi, R. C., Michelin, R. A., Neu, C. V., Nunes, H. C., Zorzo, A. F. and Kanhere, S. S. (2019). Impact of Consensus on Appendable-Block Blockchain for IoT, *16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, MobiQuitous '19, ACM, New York, NY, USA, pp. 228–237. https://doi.org/10.1145/3360774.3360798.

Lunardi, R. C., Michelin, R. A., Neu, C. V. and Zorzo, A. F. (2018). Distributed access control on iot ledger-based architecture, *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, pp. 1–7. https://doi.org/10.1109/NOMS.2018.8406154.

Lunardi, R. C., Nunes, H. C., Branco, V., Lippert, B., Neu, C. V. and Zorzo, A. F. (2019a). Performance and cost evaluation of smart contracts in collaborative health care environments, *14th International Conference for Internet Technology and Secured Transactions (ICITST-2019)*, pp. 1–6. Disponível em https://arxiv.org/abs/1912.09773.

Mertz, L. (2018). (block) chain reaction: A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution, *IEEE Pulse* **9**(3): 4–7. http://doi.org/10.1109/MPUL.2018.2814879.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here, *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3. http://doi.org/10.1109/HealthCom.2016.7749510.

Michelin, R. A., Dorri, A., Steger, M., Lunardi, R. C., Kanhere, S. S., Jurdak, R. and Zorzo, A. F. (2018). SpeedyChain: A Framework for Decoupling Data from Blockchain for Smart Cities, *15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, MobiQuitous '18, ACM, New York, NY, USA, pp. 145–154. http://doi.acm.org/10.1145/3286978.3287019.

Min, X., Li, Q., Liu, L. and Cui, L. (2016). A permissioned blockchain framework for supporting instant transaction and dynamic block size, *2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 90–96. http://doi.org/10.1109/TrustCom.2016.0050.

Moura, T. and Gomes, A. (2017). Blockchain voting and its effects on election transparency and voter confidence, *Proceedings of the 18th Annual International Conference on Digital Government Research*, dg.o '17, ACM, New York, NY, USA, pp. 574–575. http://doi.acm.org/10.1145/3085228.3085263.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, *Disponível em: https://bitcoin.org/bitcoin.pdf* .

Nunes, H. C., Lunardi, R. C., Zorzo, A. F., Michelin, R. A. and Kanhere, S. S. (2020). Context-based Smart Contracts For Appendable-block Blockchains, *Proceedings of the 2nd IEEE International Conference on Blockchain and Cryptocurrencies*, ICBC 2020, pp. 1–9. TO BE PUBLISHED.

Parizi, R. M. and Dehghantanha, A. (2018). On the understanding of gamification in blockchain systems, *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 214–219. http://doi.org/10.1109/W-FiCloud.2018.00041.

Rifi, N., Rachkidi, E., Agoulmine, N. and Taher, N. C. (2017). Towards using blockchain technology for ehealth data access management, *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)*, pp. 1–4. http://doi.org/10.1109/ICABME.2017.8167555.

Rouhani, S. and Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey, *IEEE Access* **7**: 50759–50779. http://doi.org/10.1109/ACCESS.2019.2911031.

Shahnaz, A., Qamar, U. and Khalid, A. (2019). Using blockchain for electronic health records, *IEEE Access* **7**: 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373.

Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies, *IEEE Communications Surveys Tutorials* **18**(3): 2084–2123. http://doi.org/10.1109/COMST.2016.2535718.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X. and Guizani, M. (2017). Medshare: Trust-less medical data sharing among cloud service providers via blockchain, *IEEE Access* **5**: 14757–14767. http://doi.org/10.1109/ACCESS.2017.2730843.

Zorzo, A. F., Nunes, H. C., Lunardi, R. C., Michelin, R. A. and Kanhere, S. S. (2018). Dependable iot using blockchain-based technology, *2018 Eighth Latin-American Symposium on Dependable Computing (LADC)*, pp. 1–9. https://doi.org/10.1109/LADC.2018.00010.

Zyskind, G., Nathan, O. and Pentland, A. . (2015). Decentralizing privacy: Using blockchain to protect personal data, *2015 IEEE Security and Privacy Workshops*, pp. 180–184. http://doi.org/10.1109/SPW.2015.27.