Uso de Redes Blockchain em aplicações de Metrologia e Avaliação da Conformidade

Wilson S. Melo Jr.[1], **André Ribeiro Vieira**[2] , **Raphael C. Machado**[1]
Claudio M. Farias[2], **Luiz Rust Carmo**[1]

[1] Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)
Duque de Caxias, RJ – Brasil

[2]Universidade Federal do Rio de Janeiro (UFRJ)
Programa de Pós-Graduação em Informática (PPGI) – Rio de Janeiro, RJ – Brasil

{wsjunior,rcmachado,rust}@inmetro.gov.br, {arvieira,cmfarias}@nce.ufrj.br

Abstract. *Recent works have proposed the use of blockchains in several applications related to metrology and conformity assessment. However, there are still no reports about the implementation of a blockchain network contemplating such applications. This article proposes a decentralized, permissioned blockchain network architecture that meets this need. We discuss the problems that justify the use of blockchains, detailing the proposed architecture, and describing the applications that can potentially benefit from it.*

Resumo. *Trabalhos recentes tem proposto o uso de blockchains em diversas aplicações relacionadas à metrologia e avaliação de conformidade. No entanto, não há ainda relatos práticos da implementação de uma rede blockchain contemplando tais aplicações. O presente artigo propõe uma arquitetura de rede blockchain decentralizada e permissionada que atende essa necessidade. São discutidos os problemas que justificam o uso de blockchains, os detalhes da arquitetura proposta e as aplicações que podem se beneficiar da mesma.*

1. Introdução

Blockchain é uma tecnologia emergente cujas múltiplas aplicações tem despertado a atenção de diferentes segmentos da academia, indústria, negócios e governo. Inicialmente relacionadas às criptomoedas, especialmente devido à popularidade do *Bitcoin* [Nakamoto 2008], plataformas de serviços baseados em blockchain tem sido propostas para um conjunto abrangente de aplicações [Zheng et al. 2017]. Estas incluem atividades do mercado financeiro, o setor de serviços, indústrias de diferentes segmentos [Kotobi and Bilen 2017], e mais recentemente governos e entidades representativas de interesses civis [Lee et al. 2016]. Além de introduzirem esta vasta gama de aplicações, as redes blockchain tem sido gradativamente integradas a outras tecnologias tais como redes de sensores, *smart grids*, Internet das Coisas (IoT) [Zheng et al. 2017, Christidis and Devetsikiotis 2016], entre outras.

Nos últimos meses, dois projetos científicos relacionados a pesquisas conduzidas de forma independente pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro) [Melo Jr. et al. 2019] e pelo *Physikalisch-Technische Bundesanstalt* (PTB)

[Peters et al. 2018] apresentaram a *Metrologia Legal* (ML) e a *Avaliação de Conformidade* (AC) como áreas que também podem ser beneficiadas pela tecnologia de blockchains. A Metrologia Legal [Rodrigues Filho and Gonçalves 2015] e a Avaliação da Conformidade [ISO Committee on Conformity Assessment 2014] envolvem processos essenciais para se prover confiança nas relações de consumo e prestação de serviços em qualquer sociedade desenvolvida. Somente na Europa, o valor associado à negócios que dependem essencialmente de atividades realizadas no escopo da Metrologia Legal ultrapassa a faixa dos 500 bilhões de euros/ano [Esche and Thiel 2015]. No Brasil, o Sistema Brasileiro de Avaliação da Conformidade (SBAC)[1] é responsável por processos envolvendo organismos certificadores e laboratórios de ensaio ou análises, que garantem a qualidade de mais de 250 famílias de produtos e serviços. Por se tratarem de áreas tão abrangentes, tanto a ML quanto a AC são muitas vezes alvo de ações maliciosas que visam a fraude de informações e processos. Tal prática é ainda muito comum, especialmente em países em desenvolvimento [Rodrigues Filho and Gonçalves 2015].

Nesse contexto, a tecnologia de blockchains surge como uma alternativa para prover maior confiabilidade aos processos e atividades associados à ML e à AC. Os trabalhos publicados até o momento sugerem aplicações relacionadas à auditoria de processos produtivos, segurança dos dados associados a medições e ensaios de conformidade, controle de atividades da ML envolvendo aprovação de produtos e vigilância de mercado, proteção de software, e computação distribuída para instrumentos de medição [Peters et al. 2018, Melo Jr. et al. 2019]. Entretanto, tais ideias são incompletas no sentido de não apresentarem modelos práticos para sua implementação. Tal limitação é compreensível se for considerado o fato de que soluções efetivas envolvendo blockchains são impraticáveis no escopo de uma única organização. Blockchains se baseiam na premissa de que diversas organizações independentes atuam de forma cooperativa (e.g., um consórcio composto por essas organizações) para prover determinada solução [Vukolić 2017, Zheng et al. 2017]. Partindo-se desse princípio, aplicações envolvendo casos de estudo práticos dependem da criação de uma *rede blockchain para aplicações em ML e AC* por meio do esforço integrado de diversas organizações independentes, que tenham como interesse comum o correto funcionamento dessas atividades.

O presente artigo propõe um modelo para a concepção de uma rede blockchain envolvendo Institutos Nacionais de Metrologia – do inglês, *National Metrology Institutes* (NMIs) – e demais organizações interessadas em promover soluções associadas à ML e à AC. Em linhas gerais, é descrita uma *arquitetura permissionada* [Vukolić 2017] que pode ser implementada por estas organizações de forma decentralizada e independente. Tal arquitetura não requer um sistema de administração único, exceto pela necessidade de se identificar as entidades que integram a rede blockchain. Além disso, o modelo proposto é concebido de forma a suportar múltiplas cadeias de blocos, o que permite que diferentes aplicações sejam estabelecidas entre subgrupos diferentes de organizações. Tal estratégia permite conciliar, em uma mesma rede blockchain, aplicações voltadas à pesquisa e investigação (i.e., sem o compromisso de prover um serviço permanente) e aplicações de produção que requeiram um Acordo de Nível de Serviço (ANS) entre organizações participantes e clientes.

[1] http://www.inmetro.gov.br/qualidade/

2. Contextualização

2.1. Descrição do Problema

No mundo atual, a complexidade associada aos múltiplos processos digitais introduz um desafio significativo: garantir a confiabilidade de dados e procedimentos relacionados a estes processos. Um exemplo comum ocorre quando duas partes interessadas em uma transação estabelecem um acordo e apresentam garantias quanto à sua capacidade em honrar os compromissos assumidos. No mundo digital, tal situação requer o uso de mecanismos seguros e confiáveis que atestem a integridade e autenticidade das informações providas, bem como das ferramentas efetivamente utilizados por ambas as partes.

Confiança é uma palavra intrinsecamente relacionada à ML e à AC. A ML provê a confiança nas medições de grandezas físicas em relações que envolvem o consumo de determinado bem mensurável, segurança e a proteção à vida e integridade das pessoas [Rodrigues Filho and Gonçalves 2015]. A ML se baseia diretamente em atividades que visam garantir a confiabilidade dos instrumentos de medição utilizados em diferentes aplicações. Ela é responsável, por exemplo, por promover ensaios de apreciação de modelos de instrumentos, bem como pela inspeção e fiscalização desses instrumentos posteriormente, em atividades denominadas de vigilância metrológica. A AC, por sua vez, envolve a atestação por meio de processos confiáveis de que um determinado produto satisfaz um determinado conjunto de requisitos [ISO Committee on Conformity Assessment 2014]. Para isso, é muito comum que a AC se valha de *verificações de terceira parte*, onde uma organização independente avalia um determinado produto com base em critérios pré-definidos e declara se o mesmo está em conformidade ou não.

Todavia, tal confiança tem um custo inerente. As atividades associadas à ML, por exemplo, envolvem muitas vezes uma quantidade significativa de instrumentos de medição construídos a partir de diferentes tecnologias. Consequentemente, processos como a apreciação de modelo tornam-se excessivamente caros tanto para o fabricante quanto para a sociedade. Além disso, a vigilância metrológica de um grande número de instrumentos distribuídos em grandes áreas geográficas (como é o caso do Brasil) também constitui num desafio de enormes proporções em termos de logística e capacitação de pessoal. No escopo da AC, a complexidade se dá na verificação de competência dos organismos e laboratórios responsáveis pelas atividades de avaliação de um produto. Em muitos casos, os custos envolvidos também podem representar um problema. Por fim, existe a dificuldade em se detectar e prevenir fraudes associadas aos processos de verificação de um produto, especialmente em situações onde a fraude é significativamente lucrativa a ponto de permitir inclusive o coluio entre as partes avaliadas e avaliadoras.

Na prática, os desafios apresentados estão diretamente associadas à confiabilidade de entidades que atuam nas atividades da ML e da AC, seja na verificação de um instrumento de medição ou ainda na realização de um ensaio de laboratório. Deste modo, a inevitável automatização desses processos requer também a busca de soluções inovadoras que garantam a fiabilidade e confiança do processo para todas a partes interessadas. Nesse contexto, as redes blockchain tem se mostrado uma solução atraente e promissora. As redes blockchain funcionam como um mecanismo para prover confiança entre múltiplas partes que a princípio não confiam umas nas outras [Zheng et al. 2017]. Sob esse aspecto, uma rede blockchain pode reduzir significativamente os custos associados às atividades da ML e da AC, além de prover mecanismos sofisticados para ga-

rantir a integridade e autenticidade das informações e processos gerenciados pela rede [Peters et al. 2018, Melo Jr. et al. 2019].

2.2. Como funcionam as redes blockchain

Conceitualmente, um blockchain pode ser descrito como uma estrutura de dados distribuída e apenas de escrita (denominada *ledger*) que é replicada e compartilhada entre um conjunto de *peers* de rede [Christidis and Devetsikiotis 2016]. Esta estrutura consiste em uma sequência de blocos onde o bloco n é criptograficamente ligado ao bloco $n-1$ usando uma função hash. Consequentemente, o bloco n não pode ser alterado sem modificar também todos os blocos subsequentes [Sousa et al. 2018]. Sendo um modelo descentralizado, a disponibilidade de blockchains não depende de terceiros, o que pode reduzir bastante os custos [Zheng et al. 2017]. Por sua vez, a integridade e a disponibilidade são asseguradas por consenso entre os *peers*, impedindo que toda a cadeia seja modificada e exigindo um acordo sobre qualquer bloco a ser anexado ao *ledger* [Sousa et al. 2018].

As plataformas blockchain podem ser classificadas como *não permissionadas*, quando qualquer um pode participar da rede e do protocolo de consenso, ou *permissionadas*, quando o consenso é alcançado por um conjunto de *peers* conhecidos e identificáveis [Vukolić 2017]. Geralmente, os protocolos permissionados gastam menos recursos computacionais e podem alcançar uma melhor latência de transação e *throughput* [Sousa et al. 2018]. Em contrapartida, a identificação dos *peers* em um modelo permissionado pode acarretar maior complexidade e sobrecarga de atividades associadas ao gerenciamento das identidades de cada *peer*.

Um blockchain pode armazenar virtualmente qualquer ativo digital, desde dados até *scripts* auto-executáveis, geralmente definidos como *contratos inteligentes*. Isso torna o blockchain não apenas uma arquitetura de armazenamento de dados, mas também uma plataforma completa para implementação de fluxos de trabalho automatizados e distribuídos [Christidis and Devetsikiotis 2016].

2.3. Trabalhos Relacionadas à Metrologia Legal e à Avaliação de Conformidade

Dois trabalhos publicados recentemente apresentam ideias relacionadas ao uso de blockchains para prover soluções associdas à metrologia e à avaliação de conformidade. Peters et al. [Peters et al. 2018] apresenta uma explicação detalhada sobre as redes blockchain e propõe aplicações relacionadas a auditoria descentralizada, sistemas de cobrança de tarifas, mecanismos para atualização de software Infraestruturas de Chave Pública (ICPs) para instrumentos de medição. Em uma abordagem complementar, Melo Jr. et al. [Melo Jr. et al. 2019] sugere o uso de blockchains para implementar sistemas de medição distribuídos, um conceito que traz a vantagem de simplificar a homologação, validação, verificação e supervisão metrológica de instrumentos de medição usando premissas de segurança do blockchain.

O impacto de tais ideias está essencialmente relacionado com os custos de atividades e procedimentos de segurança associados à ML e à AC. Blockchains podem automatizar e até reduzir os pontos de verificação intermediários em atividades que são muitas vezes dispendiosas. Por exemplo, o uso de contratos inteligentes para implementar software de medição legalmente relevante pode simplificar os esforços relacionados às atividades de aprovação de modelo, validação e verificação [Melo Jr. et al. 2019]. Além

disso, é possível promover a confiança entre diferentes entidades (por exemplo, fabricantes, órgãos reguladores e agentes de vigilância de mercado) sem a necessidade de uma terceira parte confiável.

3. Propondo uma Arquitetura Permissionada e Decentralizada

Neste trabalho, partimos do suposto que o uso da tecnologia de blockchain em aplicações relacionadas à ML e à AC depende da existência de uma rede (ou consórcio) composto por entidades interessadas no correto funcionamento dessas aplicações. Tal premissa é, por si só, um pré requisito para o desenvolvimento de qualquer aplicação envolvendo blockchains. Não faz sentido se falar em um blockchain composto por uma única organização. Uma rede blockchain é formada por um conjunto de *peers* providos pelas diferentes organizações que a integram.

Tão importante quanto a existência de diversas organizações, é a independência entre elas. As organizações que integram um blockchain devem ter total liberdade e responsabilidade na administração de seus respectivos *peers*. Ao mesmo tempo, as aplicações em ML e AC lidam com informações sensíveis. Deste modo, é necessário se valer de mecanismos de controle de acesso que determinem quais *peers* podem acessar quais informações em um *ledger*. Deste modo, entende-se que a rede blockchain em questão deve ser *decentralizada* (i.e., cada organização administra seus *peers* de forma independente) e *permissionada* (i.e., cada *peer* integrado à rede é autenticado por sua organização e reconhecido pelos demais *peers*).

3.1. Características de uma rede blockchain decentralizada

Conforme mencionado, a ideia de uma rede decentralizada consiste no fato de que cada organização participante é responsável pelo gerenciamento, controle e manutenção de seus *peers*. Este cenário é ilustrado na Figura 1, que descreve uma rede blockchain com três organizações independentes, onde o consenso é obtido por meio de um quorum formado por *peers* de cada uma delas. É possível observar, por exemplo, que as organizações tem total liberdade para adicionar e remover *peers*, sem a necessidade de uma coordenação centralizada. De igual modo, aplicações representadas por contratos inteligentes podem ser adicionadas e removidas, e inclusive compartilhadas entre múltiplas organizações. Para melhor compreensão das implicações decorrentes dessa forma de administração, é importante se descrever as etapas associadas à participação de uma determinada organização na rede blockchain em questão, sendo estas:

1. **Afiliação:** ocorre quando uma determinada organização passa a integrar a rede blockchain. Tal decisão pode ocorrer de forma voluntária (e.g., a organização deseja contribuir com uma aplicação de seu interesse) ou ainda por meio de acordos formais (e.g., diversas organizações estabelecem um contrato para manter uma determinada aplicação);
2. **Disponibilização de *peers*:** a organização estabelece um número determinado de *peers* com os quais contribuirá. Em linhas gerais, um *peer* corresponde a uma máquina (virtual ou física) que participa da rede blockchain, seja como um replicador de dados (i.e., o *peer* armazena e propaga os blocos que compõem o *ledger*) ou ainda como um membro do quórum de consenso. O número de peers com a qual cada organização contribui depende do formato de sua afiliação.

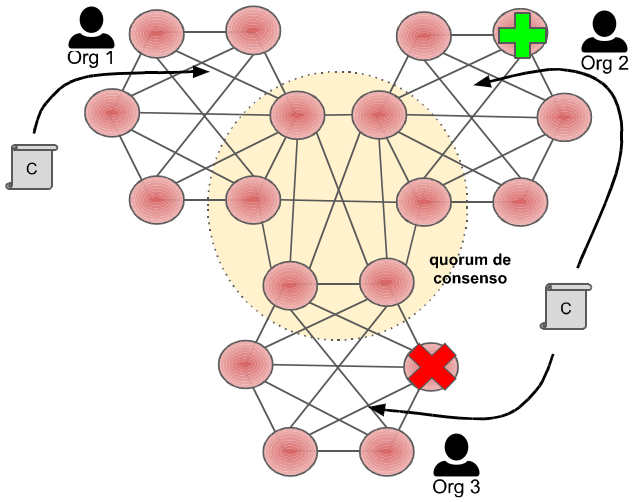

Figura 1. Exemplo de uma rede blockchain permissionada de administração descentralizada.

Organizações que integram a rede por meio de acordos formais devem disponibilizar um número específico de peers, também especificado em contrato;

3. **Identificação de *peers*:** cada organização é responsável por implementar o mecanismo de controle de acesso de seus *peers* à rede. Ao mesmo tempo, a organização deve informar aos demais participantes as respectivas credenciais de cada um de seus *peers*, de forma que eles possam ser identificados. Essa etapa será descrita em pormenores na próxima subseção;
4. **Manutenção de *peers*:** cada organização é responsável pela manutenção dos seus respectivos *peers*. Isso implica que, se um determinado *peer* se torna inoperante, a organização é responsável por seu reparo ou substituição, refazendo as demais etapas que se fizerem necessárias. Caso a afiliação seja voluntária, a organização é totalmente livre para remover ou adicionar novos *peers* sempre que julgar necessário. Entende-se que a manutenção dos *peers* é uma atividade contínua e importante para se garantir o funcionamento correto da rede blockchain; e
5. **Remoção ou revogação de *peers*:** cada organização é responsável por notificar às demais quando um *peer* é permanentemente removido da rede, ou ainda quando suas credenciais são revogadas devido a algum comprometimento de segurança.

É interessante observar que, embora as atividades associadas às etapas descritas se assemelhem em muito a atividades desempenhadas por administradores de rede, elas são na prática mais simples. Isso porque funcionalidades inerentes à tecnologia de blockchains (i.e., replicação, consenso, etc) encapsulam algumas das atividades mais críticas de uma rede blockchain. Por exemplo, uma rede blockchain não necessita de mecanismos de *backup*, uma vez que a correta replicação do *ledger* entre os *peers* já garante a recuperação do mesmo. Se um novo *peer* é adicionado na rede, ou ainda se um *peer* ativo permanece *offline* por algum tempo, o status corrente do ledger será restaurado tão logo esse *peer* se conecte aos demais.

3.2. Características de uma rede blockchain permissionada

Uma rede blockchain permissionada implica na necessidade de um mecanismo de identificação dos *peers* que compõem a rede. Ao mesmo tempo, se a rede lida com

informações sensíveis, a identificação do *peer* pode ser usada para se implementar um controle de acesso ao *ledger*.

Com relação à identificação de *peers*, o mecanismo mais adequado consiste no uso de criptografia de chave pública. Tal estratégia já existe por padrão em qualquer implementação de blockchain. Cada *peer* possui seu respectivo par de chaves (pública e privada), que deve ser o mesmo usado pela rede na autenticação de suas transações. Por sua vez, cada organização é responsável por divulgar às outras organizações as chaves públicas de seus respectivos *peers*. Um aspecto interessante é que, uma vez que se propõe uma rede decentralizada, cada organização é independente para decidir como gerenciar a atribuição de chaves criptográficas de seus *peers*. Uma organização pode, por exemplo, optar pelo uso de uma ICP para atribuição e verificação de chaves, e mesmo usar essa ICP para distribuir as chaves públicas de seus *peers* às demais organizações. Dentro do mesmo conceito, outra organização pode optar por gerenciar seus respectivos pares de chaves de forma centralizada, valendo-se de algum sistema específico (e.g. um HSM – *Hardware Security Module*) para armazenar e distribuir suas chaves de forma segura. Evidentemente, cabe a cada organização optar por um modelo cuja segurança seja adequada à aplicação.

Existe um último desafio associado ao controle de acesso ao *ledger* com base na chave pública do *peer*. Uma vez que o *ledger* é uma estrutura de dados organizada em blocos de transações, o controle de acesso a partes do *ledger* (i.e., determinadas transações podem ser acessadas e outras não) se contrapõe ao próprio mecanismo de replicação e encadeamento dos blocos. Para resolver tal problema, duas abordagens são possíveis:

- **Uso de múltiplos *ledgers***: implica no fato de que a rede blockchain gerenciará diferentes cadeias de blocos, de modo que determinadas cadeias são acessíveis a um determinado *peer*, enquanto outras não. Esta estratégia é eficiente, todavia requer o devido planejamento da aplicação, de modo a separar informações que requerem maior sigilo ou restrição de acesso em diferentes cadeias de blocos; e
- **Uso de criptografia homomórfica:** implica na criação de aplicações que encriptam qualquer informação sensível no *ledger*, todavia usando mecanismos que permitem aos demais *peers* realizarem o processamento computacional de tais informações, sem a necessidade de decriptá-las. Tal abordagem constitui uma linha interessante de investigação e um excelente exemplo de aplicação da criptografia homomórfica. No campo da ML, vale observar que o projeto *Metrology Cloud* [Oppermann et al. 2018] já prevê o uso de criptografia homomórfica para armazenamento de informações consideradas críticas em termos de privacidade.

4. Identificação de aplicações potenciais

4.1. Infraestrutura de Chave Pública para instrumentos de medição

Uma Infraestrurura de Chave Pública (ICP) é um mecanismo consolidado de gerenciamento de chaves criptográficas. Sua definição hierárquica envolvendo uma Autoridade Raiz (AR) e diversas Autoridades Certificadoras (ACs) constitui um modelo clássico de solução para aplicações que demandam o uso intensivo de diretivas criptográficas (e.g., assinatura digital). No entanto, tal solução é muitas vezes custosa, no sentido de que uma AC demanda uma série de tarefas associadas ao gerenciamento, verificação e revogação de certificados digitais, repassando esse custo aos usuários. Isso torna a ICP tradicional

uma solução pouco recomendada para cenários caracterizados pelo uso de um número grande de dispositivos de baixo custo (e.g., dispositivos IoT e instrumentos de medição).

Nesta questão, uma rede blockchain pode desempenhar um papel interessante provendo uma aplicação básica de ICP que dispensa o uso de ACs. Basicamente, a função elementar de uma AC é atestar que determinada chave pública pertence a uma respectiva entidade. No entanto, em um cenário baseado em blockchain, o fato de determinado dispositivo ter sua chave pública armazenada em um *ledger* confere aos demais participantes a garantia de que essa chave pública é imutável, o que, por sua vez, provê a irrefutabilidade sem a necessidade de um certificado digital.

Esta aplicação tem se mostrado uma necessidade essencial no âmbito dos instrumentos de medição. Diversas classes de instrumentos já utilizam criptografia assimétrica para gerar resumos criptográficos cifrados de suas medições, de modo a garantir sua integridade e autenticidade. Entretanto, pelo fato de não haver um certificado digital, não se pode garantir a irrefutabilidade de uma medição realizada por um instrumento sob controle legal (e.g., medidores de velocidade, ou ”radares”veiculares). Uma ICP baseada em blockchain supre essa lacuna de forma prática e eficiente.

4.2. Atualização de software legalmente relevante

Na literatura, o termo *legalmente relevante* é usado para designar um produto de software (ou um módulo deste) responsável pela geração ou manipulação de informações de cunho legal em instrumentos de medição controlados por software [Esche and Thiel 2015]. Fabricantes que desenvolvem software legalmente relevante para instrumentos de medição sob controle legal necessitam submeter cada nova versão do software para apreciação de modelo por uma autoridade de controle metrológico. Diferentes mecanismos podem ser empregados para garantir que um instrumento de medição receba (e aceite) apenas versões de software devidamente aprovadas. No entanto, uma forma mais efetiva de solução pode ser obtida por meio do uso de blockchains [Peters et al. 2018].

Nesta aplicação, todo instrumento de medição controlado por software é programado para buscar (e apenas aceitar) atualizações de software publicadas no blockchain. A autoridade de controle metrológico é a responsável por publicar no blockchain cada nova versão de software aprovada por ela. Ao mesmo tempo, os usuários dos dispositivos de medição podem acompanhar as atualizações de seus produtos consultando o blockchain, e assim verificar seu dispositivo está em conformidade com a última versão aprovada.

4.3. Sistemas de medição distribuídos

O desenvolvimento de sistemas que utilizam componentes computacionais remotos para executar software legalmente relevante de forma distribuída é discutida em trabalhos recentes no campo da Metrologia Legal [Oppermann et al. 2018]. Tal abordagem apresenta propriedades interessantes em contraste com arquiteturas tradicionais de instrumentos de medição, uma vez que reduz a complexidade da avaliação do software legalmente relevante, ao mesmo tempo que permite aos fabricantes desses instrumentos se valerem de tecnologias computacionais mais atuais, como, por exemplo, a virtualização e computação em nuvem. Entretanto, o uso de blockchains para a implementação desses sistemas introduz possibilidades ainda mais interessantes: o software legalmente relevante pode ser implementado como um contrato inteligente, o que transforma o blockchain em

uma ferramenta de proteção de software que auxilia a reduzir os custos associados à supervisão metrológica desses instrumentos [Melo Jr. et al. 2019].

A medição distribuída usando blockchains funciona da seguinte forma. O fabricante implementa seu instrumento de medição a partir de dois módulos básicos: um módulo de hardware seguro que realiza o sensoriamento de uma grandeza física e envia esses dados para o blockchain no formato de uma transação; e um contrato inteligente que implementa o cálculo de medição que seria realizado pelo software legalmente relevante. Após a apreciação de modelo, a autoridade de controle metrológico disponibiliza o contrato inteligente no blockchain, de modo que os módulos de hardware instalados em campo podem submeter suas transações. Todo o cálculo de medição é executado pelo próprio blockchain. Uma vez que o software legalmente relevante é um contrato inteligente escrito no *ledger*, sua integridade é garantida pelo próprio blockchain.

4.4. Gerenciamento de ensaios de proficiência e comparações interlaboratoriais

Ensaios de proficiência e comparações interlaboratoriais são métodos para avaliação do desempenho de um conjunto de participantes – laboratórios ou entidades que realizam AC – com base em critérios pré-estabelecidos. Eles constituem uma ferramenta importante na verificação da competência demonstrada por estes laboratórios na realização de testes, ensaios e experimentos necessários à avaliação da conformidade de um produto [ISO Committee on Conformity Assessment 2014]. Blockchains podem ser usados como uma plataforma eficiente para o gerenciamento de ensaios de proficiência e comparações inter laboratoriais, automatizando processos de avaliação de desempenho e provendo o armazenamento seguro das informações.

Uma forma simples de implementar tal aplicação é criando um *ledger* acessível a todos os participantes avaliados, que armazena em formato encriptado as informações referentes aos testes realizados por cada laboratório. Por exemplo, uma inter comparação laboratorial envolvendo laboratórios de medição de tempo e frequência requer que cada laboratório informe os dados de seus relógios atômicos periodicamente, para fins de comparação com os outros laboratórios. Em uma aplicação baseada em blockchain, cada laboratório escreve no *ledger* os dados referentes às suas medições, usando uma chave pública fornecida pela entidade responsável pela verificação dos resultados. Uma vez que o laboratório tenha enviado seus dados, os mesmos não podem ser mais modificados. Ao mesmo tempo, uma vez que os dados estão encriptados, os demais laboratórios não conseguem ler esses dados até que o prazo para o envio das informações seja atingido. Ao término do prazo, um contrato inteligente com acesso à chave privada referente aos ensaios é automaticamente executado pelo blockchain, decriptando todos os dados de ensaio e determinando de forma imediata o resultado da inter comparação.

5. Conclusão

Neste trabalho, foi apresentada uma arquitetura de blockchain permissionada, voltada para a criação de uma rede composta por organizações independentes e cujo gerenciamento é feito de forma decentralizada. Tal arquitetura é essencial para propiciar as aplicações aqui descritas. Estas, por sua vez, tem um impacto em potencial sobre as atividades realizadas no escopo da Metrologia Legal e da Avaliação da Conformidade. Tais resultados são importantes porque se revertem em redução de custos, simplificação de

processos e vantagens para a sociedade como um todo. Os próximos passos desse trabalho incluem a criação de um consórcio entre NMIs interessados em compor a rede blockchain. A iniciativa parte do Inmetro, e conta com o apoio do Physikalisch-Technische Bundesanstalt (PTB) e do *National Metrology Institute of Japan* (NMIJ), que são importantes NMIs no cenário internacional. Adicionalmente, algumas universidades no Brasil e em Portugal já manifestaram interesse em participar desta iniciativa, dado o potencial da mesma em prover uma plataforma real para o desenvolvimento de novos estudos e pesquisas sobre o tema.

Agradecimentos

Trabalho apoiado por CNPq, Faperj e Projeto SHCDCiber.

Referências

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4:2292–2303.

Esche, M. and Thiel, F. (2015). Software Risk Assessment for Measuring Instruments in Legal Metrology. In *Proceedings of the Federated Conference on Computer Science and Information Systems*, volume 5, pages 1113–1123.

ISO Committee on Conformity Assessment (2014). Using ISO/CASCO standards in regulations. \url{https://www.iso.org/sites/cascoregulators/index.html}.

Kotobi, K. and Bilen, S. G. (2017). Blockchain-enabled spectrum access in cognitive radio networks. In *2017 Wireless Telecommunications Symposium (WTS)*, pages 1–6.

Lee, K., James, J. I., Ejeta, T. G., and Kim, H. (2016). Electronic Voting Service Using BlockChain. *Journal of Digital Forensics, Security and Law*, 11(2):123–136.

Melo Jr., W. S., Bessani, A., Neves, N., Santin, A. O., and Carmo, L. F. R. C. (2019). Using Blockchains to Implement Distributed Measuring Systems. *IEEE Transactions on Instrumentation and Measurement*, PP(March):1–12.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Oppermann, A., Toro, F. G., Thiel, F., and Seifert, J.-P. (2018). Secure Cloud Computing: Reference Architecture for Measuring Instrument under Legal Control. *Security and Privacy*, 1(3):1–26.

Peters, D., Wetzlich, J., Thiel, F., and Seifert, J.-p. (2018). Blockchain Applications for Legal Metrology. In *IEEE International Instrumentation and Measurement Technology Conference*, page 6, Houston, Texas, USA.

Rodrigues Filho, B. A. and Gonçalves, R. F. (2015). Legal metrology, the economy and society: A systematic literature review. *Measurement*, 69:155–163.

Sousa, J., Bessani, A., and Vukolić, M. (2018). A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. In *48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*.

Vukolić, M. (2017). Rethinking Permissioned Blockchains. *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17*, pages 3–7.

Zheng, Z., Xie, S., Dai, H.-N., and Wang, H. (2017). Blockchain Challenges and Opportunities : A Survey. *International Journal of Web and Grid Services*, pages 1–24.