Auto Identificação Voluntária e Verificável de Participantes em Aplicações Baseadas em Livros-Razão Distribuídos

Marcelo Soares[1], **Rostand Costa**[2]

[1]Superintendência de Tecnologia da Informação (STI)
Universidade Federal da Paraíba (UFPB)
Caixa Postal 58.055-000 – Paraíba – PB – Brazil

[2]Laboratório de Aplicações de Vídeo Digital (LAVID)
Centro de Informática – Universidade Federal da Paraíba (UFPB)
Caixa Postal 58.055-000 – Paraíba – PB – Brazil

marcelo.soares@sti.ufpb.br, rostand@lavid.ufpb.br

Abstract. *Distributed ledger technologies have become popular through the advent of cryptocurrencies, especially Bitcoin, bringing new applicabilities and new challenges. Even though privacy and anonymity are desirable attributes of their users, there is ample evidence that, in some cases, such attributes may be dispensable and the ownership of a digital wallet address must be known. The purpose of this work is to introduce a public address-entity mapping service voluntarily populated by the owner of the wallet address, called Address Name System (ANS). A prototype of the service was implemented as a proof of concept of the proposal and the functional validation of its operations was carried out.*

Resumo. *As tecnologias de livro-razão distribuído popularizaram-se com o advento das criptomoedas, sobretudo a Bitcoin, surgindo novas aplicabilidades e novos desafios. Apesar de terem a privacidade e o anonimato como atributos desejáveis por parte dos utilizadores, há diversas evidências de que, em alguns casos, tais atributos podem ser dispensáveis, sendo necessário que a propriedade de um endereço de carteira digital seja conhecida. O objetivo deste trabalho é a propositura de um serviço público de mapeamento de endereço para entidade, alimentado voluntariamente pelo portador do endereço, chamado de Address Name System (ANS). Como prova de conceito da proposta, foi implementado um protótipo do serviço e feita a validação funcional das suas operações.*

1. Introdução

É crescente a inserção das tecnologias de informação e comunicação em nosso cotidiano. Tais tecnologias vêm se disseminando e atuando em diferentes contextos sociais. Na Engenharia de Software, um sistema evolui para atender a novos requisitos, corrigir falhas, ou mesmo se adaptar a novas tendências de mercado [Sommerville 2011]. Analogamente ao que ocorre com os sistemas de informação, a evolução das tecnologias em geral, é contínua e se adapta às tendências do ecossistema em que estão contidas, surgindo novos conceitos e novas aplicabilidades. Um exemplo disso é a verdadeira revolução que as tecnologias de livro-razão distribuído (ou DLTs, do inglês *Distributed Ledger Technologies*) estão provocando em diversos segmentos produtivos, sobretudo o financeiro, em um movimento global que se iniciou com o advento das criptomoedas, cuja primeira

concepção foi publicada em 2008 no artigo "Bitcoin: A Peer-to-Peer Electronic Cash System", por uma figura anônima que assinava com o pseudônimo Satoshi Nakamoto [Nakamoto 2008]. Nakamoto levantou a necessidade de um sistema de pagamentos baseado em uma prova criptográfica cujo o consenso é obtido através de uma rede *peer-to-peer* ao invés de uma entidade central intermediadora. A tecnologia por trás dessa abordagem foi denominada *blockchain*. Posteriormente, outras tecnologias similares foram sendo implementadas, as quais atualmente estão agrupadas genericamente sob o termo "Distributed Ledger Technology" (DLT) [Natarajan et al. 2017].

Apesar do seu surgimento ter se dado no contexto financeiro, associada à criptomoedas, as DLTs estão sendo exploradas para a utilização em diferentes tipos de aplicações. Como, basicamente, uma DLT é projetada para armazenar, de forma imutável, dados de transações, é possível expandir a sua utilização para além do contexto financeiro por meio do armazenamento de dados com outras semânticas. Campos reservados para conteúdos arbitrários [Sward et al. 2018] em diversas implementações de criptomoedas, como a **Bitcoin**[1], permitiram que usuários iniciassem experimentos utilizando tais DLTs públicas para um propósito diferente do que foi inicialmente proposto.

A atualidade do tema em questão também reflete na falta de clareza como a terminologia é empregada. Muitas vezes os termos "Distributed Ledger Technology" e "Blockchain" são usados como sinônimos, embora seja possível encontrar diferentes abordagens na implementação de DLTs que não se baseiam em *blockchain*[2] [Deshpande et al. 2017]. O mesmo ocorre com relação à identificação dos usuários. As partes envolvidas em transações são associadas a um par de chaves: chave pública e chave privada. A chave privada é utilizada para a autenticação e assinatura de transações. A partir da chave pública é derivado um identificador que representa os participantes de uma DLT. Como as principais DLTs em operação surgiram de forma associada com alguma criptomoeda, os identificadores são comumente referenciados como "endereço de carteira digital", numa alusão ao tradicional receptáculo usado para guardar dinheiro.

Como ocorre com diversas categorias de tecnologias e sistemas de informação, a evolução e o amadurecimento são dependentes de diversos aspectos, incluindo segurança. No contexto em pauta, os termos privacidade e anonimato são comumente encontrados na literatura que envolve as tecnologias de livro-razão distribuído. Para uma parte da comunidade de usuários de DLTs, o anonimato e a privacidade são atributos imprescindíveis. No entanto, diversas evidências [Costa et al. 2018, Júnior et al. 2018] apontam que, em certos cenários envolvendo aplicações baseadas em DLTs, a privacidade e o anonimato das partes envolvidas em transações podem ser dispensáveis, havendo ainda em certos casos, a identificação segura dos atores como pré-requisito para que o objetivo fim da aplicação seja alcançado.

Não é objetivo deste trabalho sugerir a quebra permanente de anonimato no ecossistema das DLTs, mas sim, propor mecanismos que permitam a convivência pacífica das aplicações que desejam privacidade com outras que precisam da identificação das partes de uma transação. Neste sentido, este artigo apresenta os resultados de um projeto de

[1]https://www.bitcoin.org

[2]Blockchain é uma implementação de DLT que usa um determinado modelo de estrutura de dados para o armazenamento de transações em blocos encadeados [Taylor et al. 2016, Natarajan et al. 2017]. Há alternativas como Tangle [Popov 2018] e Hashgraph [Baird 2016].

pesquisa focado na investigação da utilização de tecnologias consolidadas, a exemplo de certificação e assinatura digital [Stallings 2015], para o provimento de um modelo que garanta a associação confiável entre endereços de carteiras e entidades do mundo real[3].

A abordagem proposta é chamada de *Address Name System* ou ANS. O objetivo do ANS é permitir que o detentor de um endereço de carteira digital declare a sua posse voluntariamente em um padrão verificável de forma autônoma por qualquer interessado sem necessidade da intermediação de terceiros. Para a validação da abordagem proposta, foi desenvolvido um protótipo de serviço público e auto-verificável para que usuários de aplicações baseadas em DLTs possam provar e registrar a propriedade de endereços de carteiras digitais. A prova de conceito também fornece uma interface para que usuários possam consultar e validar, de forma autônoma, a propriedade de endereços de carteiras que tenham sido declaradas, independentemente da instância de DLT utilizada.

O restante deste documento está estruturado da seguinte forma: na Seção 2 é feita uma discussão sobre privacidade e anonimato em DLTs, com foco na problemática a ser tratada neste trabalho. A Seção 3 apresenta a solução proposta, descrevendo a sua especificação e abordagem para a resolução do problema. A Seção 4 apresenta a prova de conceito implementada para validar a estratégia proposta. A Seção 5 traz alguns trabalhos relacionados e, por fim, a Seção 6 traz as considerações finais e sugestões para trabalhos futuros.

2. Privacidade em DLTs

Atualmente, podemos encontrar aplicações apoiadas nos livros-razão distribuídos em diferentes áreas, das quais podemos citar [Taylor et al. 2016, Lemieux et al. 2018]: aplicações notariais, saúde, indústria, agricultura, telecomunicações, etc. A Figura 1 representa uma abstração arquitetural de alto nível sobre aplicações apoiadas em livros-razão distribuídos. O potencial das DLTs aliado a sua flexibilização na utilização em diversos segmentos, vêm atraindo o interesse de governos de vários países para a exploração dessa nova tecnologia em direção ao provimento de serviços à sociedade [Dhar and Bose 2016, Taylor et al. 2016, Deshpande et al. 2017, Maltese 2015]. Na América do Sul, o Brasil se tornou o primeiro país a realizar uma prova de conceito bem sucedida na utilização de DLT pelo governo, através do desenvolvimento de um sistema de verificação de documentos de identidade [Bakker 2018].

Em geral, os termos privacidade e anonimato estão automaticamente incluídos dentro do escopo da utilização de DLTs. Normalmente, o modelo de funcionamento das criptomoedas tenta prover o anonimato dos atores envolvidos, e por consequência, a privacidade em suas ações. Ainda que Nakamoto não tenha mencionado a motivação para a necessidade de privacidade em uma DLT, é possível encontrar na literatura colocações que sugerem a importância do anonimato. Tennant menciona que, sem a privacidade, informações confidenciais poderiam ser vazadas, assim como transações para IOT (do inglês *Internet of Things*) poderiam ser monitoradas para o planejamento de roubos [Tennant 2017]. Conforme citado por Nakamoto, em um modelo bancário tradicional, um certo nível de privacidade é alcançada mantendo a informação entre as partes envolvidas em uma transação e uma entidade terceira confiável [Nakamoto 2008]. Para um

[3]Os termos "entidade do mundo real" ou "pessoa/entidade" serão usados para fazer referência à uma pessoa física ou jurídica que tenha a posse de algum certificado digital válido.

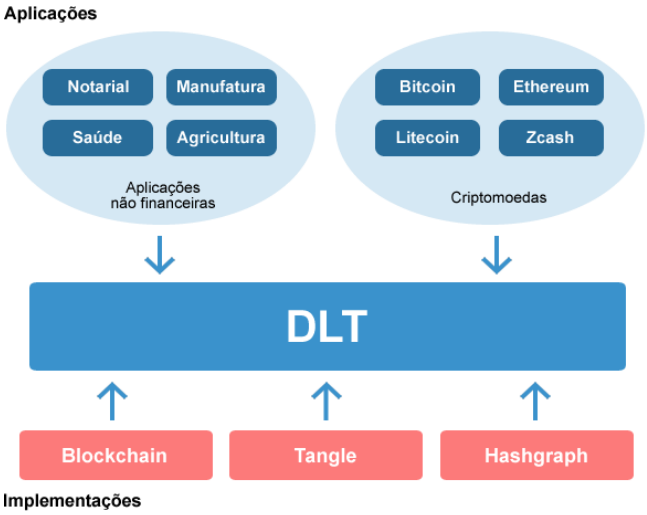

Figura 1. Aplicações em DLTs

cenário onde as transações devem ser públicas, a privacidade pode ser alcançada mantendo anônima a propriedade de uma chave pública. Nesse contexto, o termo pseudônimo digital é frequentemente usado para designar uma chave pública associada a uma chave privada de propriedade desconhecida [Narayanan and Clark 2017].

Mas será que o modelo de utilização de criptografia de chave pública para que os usuários possam transacionar em uma DLT realmente provê um anonimato completo?

Desde a primeira concepção de DLT, já era sugerida a utilização de vários pares de chaves em transações distintas para evitar a quebra do anonimato [Nakamoto 2008]. É comum encontrar trabalhos que investigam o anonimato e privacidade em DLTs. Reid e Harrigan concluem que, por meio de ferramentas apropriadas, é possível associar muitas chaves públicas umas às outras e monitorar a atividade de usuários da rede [Reid and Harrigan 2011]. Meiklejohn et al. apresenta uma heurística de *clustering* baseada em endereços de mudança, que permite agrupar endereços pertencentes ao mesmo usuário [Meiklejohn et al. 2013]. Ainda no ambiente de criptomoedas, o detentor de ativos digitais está sujeito a trocar os seus valores por moedas reais, como o dólar ou euro. Para tal, o usuário deverá interagir com um sistema de câmbio, que poderá aplicar as suas regras de conhecimento do cliente [Taylor et al. 2016]. Uma simples compra de produtos em um e-commerce já seria o suficiente para que o anonimato de quem está por trás do endereço da carteira seja quebrado e sua identidade seja revelada. Tais estudos nos levam a concluir que o anonimato em DLTs é, na verdade, um pseudo-anonimato. A própria comunidade Bitcoin alerta em sua página que a criptomoeda não é anônima, já que a privacidade é mantida apenas no escopo da rede descentralizada [Bitcoin 2018].

Muitos estudos e pesquisas direcionam os seus esforços na busca por métodos para prover o anonimato pleno, e, consequente, a privacidade plena. É importante salientar que, em um contexto financeiro, o anonimato pleno dos atores envolvidos em transações pode facilitar o uso para atividades criminosas [Möser and Böhme 2017]. Em 2013, o FBI fechou um website que funcionava como um comércio de drogas ilegais e já havia movimentado cerca de 1,3 bilhão de dólares com pagamentos feitos em Bitcoin [Pagliery 2013]. Mais recentemente, em 2017, um ataque em escala mundial de um ran-

somware conhecido como *WannaCry* sequestrou dados de mais de 45 mil computadores em 74 países, de acordo com a empresa russa de segurança Kaspersky [Perekalin 2017]. Mais uma vez, a criptomoeda Bitcoin esteve associada aos ataques por ser o meio indicado pelos invasores para o pagamento de um "resgate" dos dados sequestrados. Por sua associação constante à ataques e a sites da rede dark/deep web, a Bitcoin é alvo de desconfiança por parte da sociedade [Taylor et al. 2016].

Claramente há inúmeros desafios associados com a garantia de anonimato e privacidade, sobretudo nas DLTs públicas. Mas, e quando o anonimato é explicitamente dispensado?

Uma das principais criptomoedas em operação, a Bitcoin, disponibiliza em seu site o endereço da carteira digital de propriedade da comunidade mantenedora da criptomoeda (Figura 2). Também é comum encontrar páginas de comércio eletrônico exibindo os seus endereços de carteiras com representação em QR Code. Uma simples divulgação de endereço com fins de arrecadar fundos nos leva a refletir sobre a necessidade de identificação das entidades por trás dos endereços de carteiras digitais. Nota-se que, mesmo em um contexto financeiro envolvendo uma criptomoeda, não há preocupação com o anonimato de uma das partes envolvidas. Uma invasão ao sistema gerenciador de conteúdo do website oficial da Bitcoin com a alteração do endereço de carteira exibido resultaria em milhares de pessoas enviando fundos, sem conhecimento, para um terceiro malicioso.

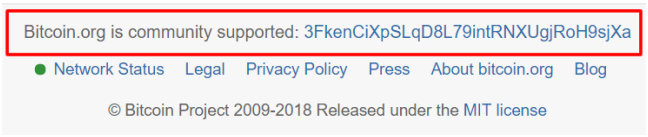

Figura 2. Endereço de Carteira no Site bitcoin.org

Também é possível encontrar ocorrências de programas maliciosos que atuam de forma a manipular a área de transferência do sistema operacional, com o intuito de alterar o endereço de destino de uma transação que foi copiado pelo usuário do sistema. Como os softwares de carteira[4] não apresentam qualquer informação sobre o proprietário do endereço de destino, os fundos são transferidos erradamente para um outro receptor, sem que o remetente perceba [Rashid 2014].

Neste sentido, tanto a garantia do anonimato de quem deseja quanto a legitimidade da declaração de posse de um endereço de carteira digital são relevantes e desejáveis no contexto de DLTs. Este trabalho foca no segundo caso.

3. Address Name System: Permitindo a Declaração Voluntária de Posse de Endereços de Carteiras Digitais

A solução proposta e descrita nesta seção é dividida em dois módulos principais. Um módulo para registro, a ser utilizado de maneira voluntária por parte do detentor de um endereço de carteira e de um certificado digital para registrar o mapeamento de endereço para entidade (ou endereço-entidade), e um módulo de consulta, que em uma visão mais

[4]Softwares clientes responsáveis por gerenciar o acesso a endereços e auxiliar na realização de transações em DLTs.

ampla, corresponde a um serviço que recebe parâmetros de entrada como um identificador de uma instância de DLT e um endereço de carteira e retorna ao usuário a identidade declarada, se houver uma. Por ter o funcionamento semelhante ao do consolidado serviço de tradução de nomes em recursos, *Domain Name System* (DNS), utilizou-se a nomenclatura *Address Name System* (ANS) para fazer referência ao serviço proposto neste trabalho.

Em uma visão geral, o mapeamento deve ser feito de forma que seja possível comprovar a identidade de uma pessoa/entidade, e comprovar que essa pessoa/entidade é proprietária da chave privada de um determinado endereço. Este mapeamento é feito através de dois passos: i) **prova de posse** e ii) **prova de identidade**. A **prova de posse** do endereço de carteira indica se a pessoa/entidade possui acesso ao endereço de carteira para transacionar em uma DLT. A comprovação de posse é feita com a assinatura digital de uma estrutura de dados utilizando a chave privada correspondente à chave pública do endereço reivindicado. A **prova de identidade** tem como objetivo obter a comprovação de que quem está pedindo a associação é quem diz ser e é feita com a assinatura digital realizada com a chave associada a um certificado digital[5]. Neste sentido, um pré-requisito para o registro no ANS é que a pessoa/entidade possua um certificado digital válido e uma premissa para a confiabilidade do mapeamento é que uma Autoridade Certificadora (AC) tenha realizado os procedimentos de verificação de documentos corretamente, obtendo êxito na emissão correta do certificado. Uma premissa fundamental do ANS é que tais provas sejam autocontidas e possam ser verificadas de forma autônoma por qualquer interessado em qualquer tempo.

Entretanto, caso utilizadas separadamente, as assinaturas para prova de posse e prova de identidade não fariam qualquer associação entre os proprietários de suas respectivas chaves. É necessária, portanto, a vinculação entre a prova de posse do endereço e a prova de identidade de modo a garantir que o proprietário da chave privada de acesso ao endereço de carteira é o mesmo proprietário da chave privada que o identifica através do certificado digital. Esta associação é feita com o uso de um documento XML específico, chamado de **ANS Certificate**. A estrutura do **ANS Certificate** (Figura 3) é baseada na estrutura de um certificado digital X.509[6], com uma seção de dados a serem assinados, um algoritmo de assinatura e a assinatura digital [Housley et al. 2002]. Ela foi modelada para fazer referência tanto ao certificado digital do usuário quanto ao endereço da carteira. Para referenciar o certificado digital, o documento contém os campos *Distinguished Names*[7] da AC emissora e o *serial number* do certificado, que o identifica unicamente dentre os certificados emitidos por uma AC. Tais atributos são agrupados no elemento $< EntityCertificate >$ da seção $< ToBeSigned >$, como pode ser visto na Figura 3.

Além dos dados de referência ao certificado da pessoa/entidade, a seção $< ToBeSigned >$ de um **ANS Certificate** contém ainda os atributos $< DLTInstance >$, $< Address >$, e $< ExpirationDate >$, onde os dois primeiros especificam a instância da DLT e o endereço da carteira, respectivamente, e o último indica a data de validade do **ANS Certificate**. Há ainda o elemento $< DLTSignature >$

[5]No Brasil, um documento eletrônico assinado por uma chave emitida por uma AC da cadeia ICP-Brasil possui validade jurídica [Brasil 2001].

[6]Padrão internacional de certificado utilizado pela ICP-Brasil [Housley et al. 2002] [ITI 2018].

[7]*Distinguished names* são estruturas compostas por atributos. Alguns atributos que podem ser encontrados dependendo da implementação da infraestrutura são: *country, organization, organizational-unit, distinguished name qualifier, state or province name, common name* [Housley et al. 2002].

```
▼<ANSCertificate>
 ▼<ToBeSigned>
    <DLTInstance>Bitcoin</DLTInstance>
    <Address>1731jmNNp7rTur9UhpGeDK1BkaJVManUsd</Address>
   ▼<EntityCertificate>
     <Type>X.509</Type>
    ▼<Issuer>
       <C>BR</C>
       <O>ICP-Brasil</O>
       <OU>Secretaria da Receita Federal do Brasil - RFB</OU>
       <CN>AC Certisign RFB G5</CN>
     </Issuer>
     <SerialNumber>113229039 ———————— 4891971238</SerialNumber>
   </EntityCertificate>
   <ExpirationDate>2019-08-02 20:15:07</ExpirationDate>
 </ToBeSigned>
▶<DLTSignature xmlns="http://www.———————— /xmldltsig#">...</DLTSignature>
▶<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">...</Signature>
</ANSCertificate>
```

Figura 3. Exemplo de um ANS Certificate

usado para armazenar a assinatura digital usada como prova de posse e, finalmente, o elemento $< \ Signature \ >$, usado para armazenar a assinatura digital usada em nosso contexto como prova de identidade. As assinaturas são acrescentadas ao final do documento conforme a estratégia de assinatura envelopada[8] [Bartel et al. 2015]. O elemento $< Signature >$ utiliza a estrutura em conformidade com o consolidado padrão internacional W3C, que armazena além da assinatura digital, o certificado associado à chave privada utilizada [Bartel et al. 2015]. O elemento $< DLTSignature >$ contém o algoritmo usado para a assinatura, a chave pública referente ao endereço de carteira e a assinatura digital, conforme modelado no *XML Schema Definition* (XSD) e apresentado na Figura 4.

```
▼<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" version="1.0.0">
 ▼<xs:element name="DLTSignature">
   ▼<xs:complexType>
    ▼<xs:sequence>
       <xs:element name="Algorithm" type="xs:string"/>
       <xs:element name="PublicKey" type="xs:string"/>
       <xs:element name="SignatureValue" type="xs:string"/>
     </xs:sequence>
   </xs:complexType>
 </xs:element>
</xs:schema>
```

Figura 4. *XML Schema Definition* do Elemento DLTSignature

Conforme descrito anteriormente, a estratégia adotada para o mapeamento basicamente utiliza a combinação de assinaturas digitais. A pessoa/entidade inicialmente assina digitalmente a seção $< \ ToBeSigned \ >$ do **ANS Certificate** com a chave privada do endereço e, em seguida, tanto a seção $< \ ToBeSigned \ >$ quanto a seção $< \ DLTSignature \ >$ são assinadas com a chave privada do certificado, gerando um pacote que contém o **ANS Certificate** duplamente assinado, a chave pública associada ao endereço para a verificação da prova de posse e o certificado digital com a respectiva chave pública para a verificação da prova de identidade. Como a assinatura para a prova de identidade é feita com a chave privada do certificado digital que é referenciado no próprio documento, é formado um elo entre a prova de posse do endereço de carteira e a prova de identidade. Este fluxo está ilustrado na Figura 5.

[8]Na estratégia de assinatura *Enveloped*, o conteúdo da assinatura é o próprio documento XML e o valor da assinatura é inserido ao final do documento juntamente com o certificado digital do assinante, gerando um artefato final que contém todos os elementos necessários para a verificação de autenticidade da informação criptografada [Bartel et al. 2015].

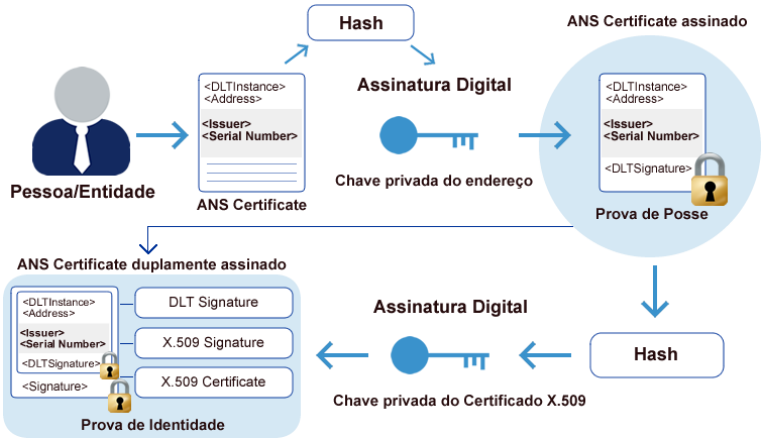

Figura 5. Fluxo de Assinatura de um ANS Certificate

A validação das assinaturas e, consequentemente, da associação entre pessoa/entidade e endereço de carteira, é feita em um processo inverso que usa as respectivas chaves públicas do certificado digital e do endereço de carteira. Tal verificação se baseia em procedimentos bem estabelecidos com algoritmos públicos e padronizados e pode ser feita de forma autônoma a partir do próprio **ANS Certificate**, o qual é um pacote autocontido contendo todos os artefatos necessários para que um interessado possa verificar a autenticidade das informações. Deste modo, utilizando a chave pública contida no certificado digital utilizado, é possível conferir a autenticidade da prova de identidade, e associar o **ANS Certificate** ao proprietário do certificado. Da mesma forma, é possível verificar a assinatura digital da prova de posse utilizando a chave pública do endereço de carteira e associar o **ANS Certificate** ao proprietário do endereço. A Figura 6 ilustra o fluxo para a verificação das provas necessárias para a validação da associação endereço-entidade.

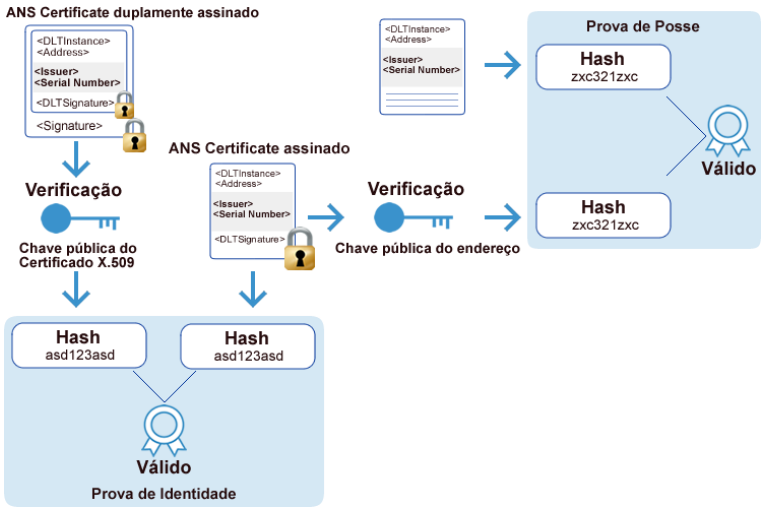

Figura 6. Fluxo de Verificação de um ANS Certificate

Para completar o mecanismo proposto, é necessário disponibilizar uma forma de que os **ANS Certificates** autoproduzidos pelos detentores dos endereços possam ser facilmente recuperados por qualquer parte interessada. Uma forma tradicional de fazer isso

é através de uma rede hierárquica de repositórios, similar ao que ocorre com o DNS. No caso do ANS, um repositório padrão (equivalente a um *default gateway* do DNS) pode ser usado como primeira referência para recuperação de um **ANS Certificate** relacionado com um dado endereço de carteira digital, caso tenha sido produzido. Cada repositório, por sua vez, também possui o seu próprio *default gateway* e assim por diante, até chegar em um repositório raiz. As requisições são então checadas na base local e, caso não exista, são propagadas para o nível seguinte até atingir o último nível. A resposta para uma solicitação é o próprio **ANS Certificate**, caso encontrado, ou uma indicação que o endereço em pauta ainda não possui declaração de propriedade. A inclusão (ou registro) de um novo **ANS Certificate** na rede de repositórios segue um fluxo similar, exceto que sempre atinge o repositório raiz. Uma cópia do novo **ANS Certificate**, após validada, é armazenada em cada repositório por onde passar durante o seu registro.

4. Prova de Conceito: Um Protótipo Funcional do ANS

Para demonstrar a viabilidade de implementação de um serviço de resolução da relação entre endereços de carteiras digitais e pessoas/entidades seguindo a abordagem proposta, foi construído um protótipo totalmente funcional do ANS. O protótipo desenvolvido é composto de dois componentes: um repositório de **ANS Certificates** registrados e uma aplicação cliente, responsável tanto pela geração e submissão de novos **ANS Certificates** quanto pela recuperação de **ANS Certificates** a partir de endereços de carteiras.

A aplicação chamada de **ANS Client** foi desenvolvida para representar a interface no lado do cliente, contemplando os processos realizados por qualquer aplicação cliente que possa ser integrada. O **ANS Client** obtém os dados necessários para a produção de um **ANS Certificate**, formata o arquivo XML equivalente, faz as assinaturas digitais conforme descrito na Seção 3 e envia o **ANS Certificate** gerado para registro em um servidor ANS, chamado **ANS Server**. O **ANS Server** desenvolvido no protótipo é um repositório de **ANS Certificates** implementado como um serviço web e acessível através de uma *API RESTful*. A arquitetura geral do protótipo está ilustrada na Figura 7.

Para iniciar um registro de propriedade de um endereço de carteira digital, a pessoa/entidade deverá informar no **ANS Client** a instância de DLT na qual o endereço foi criado, a chave privada do endereço de carteira, os dados de acesso ao *keystore*[9] onde a chave privada do certificado foi instalada e o seu respectivo certificado digital, conforme pode ser visto nas telas mostradas na Figura 8. O endereço de carteira é derivado a partir de um hash da chave pública[10] correspondente à chave privada informada, sendo calculado pelo **ANS Client** e exibido em tela.

O **ANS Server** conduz o processo de registro de um novo **ANS Certificate** aplicando as verificações necessárias para a garantia da legitimidade do mapeamento endereço-entidade. Basicamente, são realizadas as seguintes tarefas: validação das assinaturas com as respectivas chaves públicas, verificação do elo entre as duas provas,

[9]Nesta primeira versão do protótipo foi utilizado um certificado digital ICP-Brasil do tipo A1, que é um certificado disponibilizado ao usuário como um arquivo digital para que seja instalado no computador.

[10]Na plataforma Ethereum, o endereço de carteira é formado pelos 160 bits mais a direita do resultado de uma função hash Keccak-256 da chave pública [Wood 2017]. Na Bitcoin, o endereço possui tamanho de 160 bits e é formado a partir do uso combinado de diferentes funções de hash (RIPEMD-160 e SHA-256) [Bitcoin-Wiki 2018].

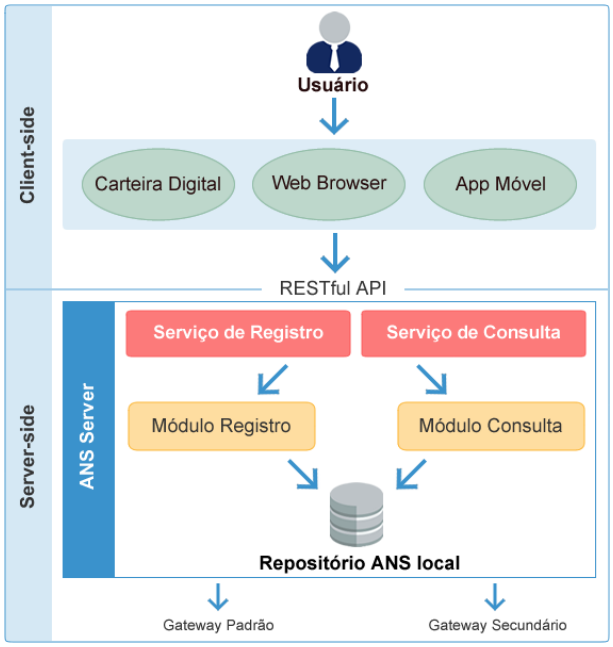

Figura 7. Arquitetura do Protótipo

inserção de um registro em sua tabela de mapeamento e armazenamento do **ANS Certificate** em seu repositório local. Caso o **ANS Server** esteja ligado a uma outra instância, o novo **ANS Certificate** é repassado e novamente validado e armazenado no **ANS Server** seguinte. Este repasse continua até que seja atingido um **ANS Server** raiz.

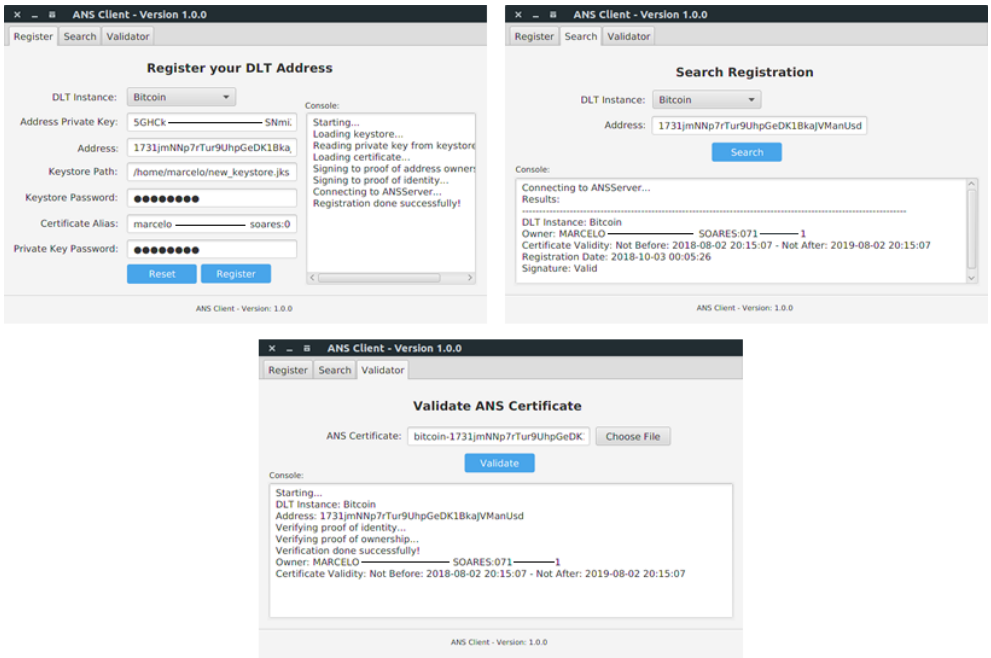

Figura 8. Telas do Protótipo: ANS Client

A recuperação padrão de **ANS Certificates** também é feita através da uma *API RESTful*, permitindo a integração com *softwares* de carteiras digitais e outras aplicações, inclusive aplicativos para dispositivos móveis. Ao receber uma solicitação de consulta,

o **ANS Server** pesquisa no seu repositório a partir dos parâmetros informados e também consulta o seu **ANS Server** secundário caso não encontre o **ANS Certificate** localmente. Caso o **ANS Certificate** seja encontrado em algum repositório, o **ANS Server** de entrada realiza toda a validação das assinaturas novamente antes de devolver o **ANS Certificate** para o solicitante.

O **ANS Server** do protótipo também fornece uma interface web para que um interessado possa obter um **ANS Certificate** de forma interativa. A interface fornece campos para que o usuário informe a instância da DLT e o endereço da carteira e, caso haja o **ANS Certificate**, os dados do mesmo são exibidos para o solicitante. Para uma maior confiabilidade, a interface web também disponibiliza a opção de fazer *download* do **ANS Certificate** para que o usuário possa fazer o processo de verificação de forma autônoma, caso deseje. Também é possível exportar e fazer o *download* do certificado digital X.509 contido no **ANS Certificate** para a verificação da identidade da pessoa/entidade associada ao endereço. Tal interface é mostrada na Figura 9.

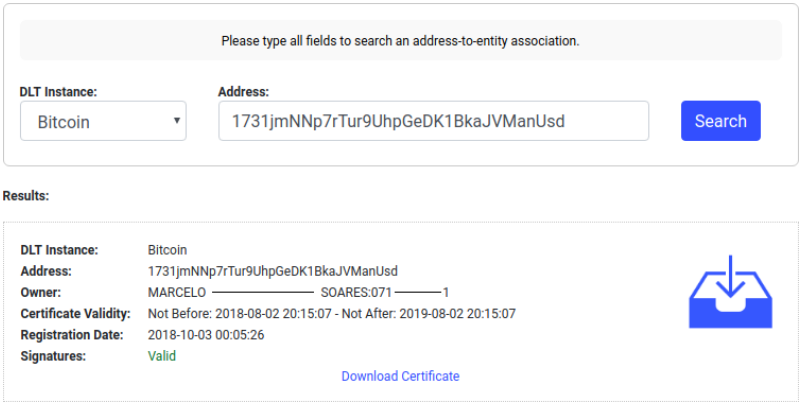

Figura 9. Protótipo: Interface Interativa do ANS Server

5. Trabalhos Relacionados

Desde as sua primeiras implementações até os dias atuais, as DLTs são exploradas por uma gama de aplicações e comunidades, onde a privacidade e anonimato são atributos desejáveis por parte dos usuários. No entanto, embora estejam surgindo evidências de que o anonimato pode, em alguns casos, ser dispensável, ainda há uma lacuna na literatura acerca de propostas de soluções para o mapeamento de endereços de carteiras e seus respectivos proprietários. Os casos abaixo, ambos no Brasil, ilustram essa demanda.

Júnior et al. explícita um cenário onde há a necessidade de associação entre endereços de carteiras e entidades do mundo real [Júnior et al. 2018]. O referido trabalho apresenta uma proposta de criação de uma representação de um ativo digital apelidado de BNDSToken, em uma infraestrutura de blockchain para rastrear os recursos do Banco Nacional de Desenvolvimento Econômico e Social. Uma das premissas da proposta é que apenas pessoas jurídicas detentoras de um certificado digital e-CNPJ[11] podem receber o BNDSToken. Os autores citam como um pré-requisito para a implementação da proposta, a existência de um serviço que forneça o mapeamento entre endereços de carteiras em uma blockchain e pessoas jurídicas do Brasil.

[11]Nome dado a um certificado digital e sua respectiva chave emitidos pela ICP-Brasil que representam eletronicamente uma pessoa jurídica do Brasil.

Costa et al. também apresenta um serviço que demanda que as partes envolvidas sejam identificadas de uma forma segura para dar legitimidade as transações [Costa et al. 2018]. O serviço, chamado de RAP, combina o uso de DLTs, certificação digital e preservação digital para a criação de uma plataforma, escalável e agnóstica, especializada no registro, autenticação e preservação de documentos digitais. Como prova de conceito da plataforma proposta, foi feita a construção de um serviço público para registro e verificação digital da autenticidade de documentos acadêmicos. No protótipo, o registro dos diplomas acadêmicos pode ser feito em duas das DLTs mais populares, *Bitcoin* e *Ethereum*, através de uma transação entre a carteira da instituição emissora (uma IES) e a carteira da instituição autenticadora (RNP ou MEC, por exemplo). Neste caso, a publicização inequívoca da propriedade dos endereços de carteiras digitais em pauta poderia garantir a transparência e a segurança das transações de registro.

6. Conclusão

Durante o desenvolvimento deste trabalho foi possível observar a dinâmica na evolução das tecnologias de livro-razão distribuído e entender que a sua capacidade de adaptação em diferentes contextos traz também novos desafios. Percebeu-se que o anonimato e a privacidade em determinadas situações podem ser dispensados, abrindo uma grande lacuna para a investigação de soluções que possam ajudar a identificar, legítima e inequivocamente, as entidades por trás de endereços de carteiras digitais.

Neste sentido, a abordagem apresentada propôs a utilização de tecnologias e conceitos consolidados nas próprias DLTs para a resolução de um problema específico. O mecanismo proposto pode ser utilizado por aplicações onde é necessária a identificação dos atores envolvidos em transações de forma não exclusiva e com suporte a múltiplas instâncias de DLTs. O protótipo desenvolvido como prova de conceito ajudou a demonstrar a viabilidade da declaração espontânea de uma relação endereço-entidade como também a sua recuperação e verificação de forma independente através de uma rede cooperativa de repositórios abertos e da validação de assinaturas digitais. Segundo a IDC, espera-se que o gasto anual com DLTs chegue a 9,7 bilhões de dólares em 2021 [IDC 2018], o que sugere também o crescimento de aplicações que necessitem da identificação dos seus participantes. Neste cenário, o ANS se apresenta como um serviço de grande utilidade para a comunidade de desenvolvedores e usuários de aplicações baseadas em DLTs que dispensam o anonimato.

Há várias etapas e desafios a serem vencidos para o amadurecimento da proposta do ANS e o lançamento de uma versão de referência do serviço. Neste sentido, os próximos passos da pesquisa incluem:

- Integração do ANS em *softwares* populares de carteira digital;
- Integração do ANS em sites de visualização de transações em DLTs (como o **Block Explorer**[12], por exemplo);
- Suporte à certificados em tokens ou cartões;
- Implementar a replicação e sincronismo da rede de repositórios;
- Permitir a revogação de **ANS Certificates**;
- Estruturar a abertura do código do ANS para viabilizar a sua manutenção e evolução.

[12]https://live.blockcypher.com

Referências

Baird, L. C. (2016). The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance. Technical Report SWIRLDS-TR-2016-01, Swirlds, Inc.

Bakker, E.-J. (2018). Brazil's beginning blockchain business.

Bartel, M., Boyer, J., Fox, B., LaMacchia, B., and Simon, E. (2015). Xml signature syntax and processing. https://www.w3.org/TR/xmldsig-core2/. [Online; accessed 05-August-2018].

Bitcoin (2018). Some things you need to know. https://bitcoin.org/en/you-need-to-know. [Online; accessed 04-August-2018].

Bitcoin-Wiki (2018). Technical background of version 1 bitcoin addresses. https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses. [Online; accessed 05-August-2018].

Brasil (2001). Medida provisória no 2.200-2, de 24 de agosto de 2001.

Costa, R., Faustino, D., Lemos, G., Queiroga, A., Djohnnatha, C., Alves, F., Lira, J., and Pires, M. (2018). Uso não financeiro de blockchain: Um estudo de caso sobre o registro, autenticação e preservação de documentos digitais acadêmicos. *Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain-SBRC)*, 1(1/2018).

Deshpande, A., Stewart, K., Lepetit, L., and Gunashekar, S. (2017). Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards. Technical report, British Standards Institution (BSI).

Dhar, S. and Bose, I. (2016). Smarter banking: Blockchain technology in the indian banking system. *Asian Management Insights*, 3:46–53. https://ink.library.smu.edu.sg/ami/3.

Housley, R., Polk, T., Ford, D. W. S., and Solo, D. (2002). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280. https://rfc-editor.org/rfc/rfc3280.txt. [Online; accessed 04-August-2018].

IDC (2018). New idc spending guide sees worldwide blockchain spending growing to $9.7 billion in 2021. https://www.idc.com/getdoc.jsp?containerId=prUS43526618. [Online; accessed 04-August-2018].

ITI (2018). Glossário - instituto nacional de tecnologia da informação - iti. http://www.iti.gov.br/glossario. [Online; accessed 04-August-2018].

Júnior, G. M. A., Jr., J. N. D., Onodera, M. T., de Borba Maranhão Moreno, S. M., and da Rocha Santos Almeida, V. (2018). Bndestoken: Uma proposta para rastrear o caminho de recursos do bndes. *Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain_SBRC)*, 1(1/2018).

Lemieux, V., Flores, D., and Lacombe, C. (2018). Real estate transaction recording in the blockchain in brazil (rcplac-01) - case study 1.

Maltese, M. E. G. (2015). Singapore prime minister said national banks can use blockchain. https://cointelegraph.com/news/singapore-prime-minister-said-national-banks-can-use-blockchain. [Online; accessed 04-August-2018].

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 127–140, New York, NY, USA. ACM.

Möser, M. and Böhme, R. (2017). The price of anonymity: empirical evidence from a market for bitcoin anonymization. *Journal of Cybersecurity*, 3(2):127–135.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Narayanan, A. and Clark, J. (2017). Bitcoin's academic pedigree. *Commun. ACM*, 60(12):36–45.

Natarajan, H., Krause, S., and Gradstein, H. (2017). Distributed ledger technology (dlt) and blockchain. FinTech note; no. 1. Washington, D.C. : World Bank Group. http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain. [Online; accessed 06-August-2018].

Pagliery, J. (2013). Fbi shuts down online drug market silk road. https://money.cnn.com/2013/10/02/technology/silk-road-shut-down/index.html. [Online; accessed 04-August-2018].

Perekalin, A. (2017). How to protect vs. wannacrypt. https://www.kaspersky.com/blog/wannacry-ransomware/16518/. [Online; accessed 04-August-2018].

Popov, S. (2018). The tangle. https://iota.org/IOTA_Whitepaper.pdf. [Online; accessed 02-August-2018].

Rashid, F. Y. (2014). A closer look at how criminals steal your bitcoins, and how to stop them. https://www.itproportal.com/2014/03/08/a-closer-look-at-how-criminals-steal-your-bitcoins-and-how-to-stop-them/. [Online; accessed 04-August-2018].

Reid, F. and Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. *ArXiv e-prints*.

Sommerville, I. (2011). *Software Engineering*. Ninth Edition, 9 edition.

Stallings, W. (2015). *Criptografia E Segurança De Redes*. PEARSON BRASIL.

Sward, A., Vecna, I., and Stonedahl, F. (2018). Data insertion in bitcoin's blockchain. *Ledger*, 3(0). https://ledgerjournal.org/ojs/index.php/ledger/article/view/101/91. [Online; accessed 10-September-2018].

Taylor, S., Brown, R. G., Lehdonvirta, V., Ali, R., Sasse, A., Godsiff, P., Godsiff, P., Mulligan, C., and Curry, P. (2016). Distributed ledger technology: beyond block chain. Technical report, Government Office for Science.

Tennant, L. (2017). Improving the anonymity of the iota cryptocurrency. http://iotafeed.com/wp-content/uploads/2017/08/anonymity-iota.pdf. [Online; accessed 21-September-2018].

Wood, G. (2017). Ethereum: A secure decentralised generalised transaction ledger eip-150 revision (759dccd - 2017-08-07). https://ethereum.github.io/yellowpaper/paper.pdf. [Online; accessed 04-August-2018].