Abordagem Taxonômica Voltada às Aplicações Baseadas em Identidades Digitais Descentralizadas

Anália Cristina B. T. Meira[1], Anderson B. Morte[1], Dênio Mariz[1], Rostand Costa[2]

[1]Instituto Federal da Paraíba (IFPB)
Caixa Postal 15.064 – 91.501-970 – João Pessoa – PB – Brasil

[2]Laboratório de Aplicações de Vídeo Digital (LAVID) –
Universidade Federal da Paraíba (UFPB)
Rua dos Escoteiros, s/nº – Mangabeira, João Pessoa – PB – Brasil

{analia.meira,vieira.anderson}@academico.ifpb.edu.br,

denio@ifpb.edu.br, rostand.lavid.ufpb.br

Abstract. *A decentralized digital identity system brings in its scope principles such reliability, high scalability and security. This article focuses on providing a study on Identity Management models, to deal with the challenges found in traditional models, such as privacy and security. We present a decentralized digital identity taxonomy based on blockchain, whose purpose is to be used to promote the autonomy and control of data by the user. Finally, we analyze two popular blockchain-based systems: uPort and sovrin, in order to assist software designers interested in evaluating the most appropriate mechanism.*

Resumo. *Um sistema de identidade digital descentralizado traz em seu escopo princípios como confiabilidade, alta escalabilidade e segurança. Este artigo apresenta um estudo sobre modelos de Gerenciamento de Identidades para lidar com desafios encontrados nos modelos tradicionais, como a privacidade e segurança. Apresenta uma taxonomia de identidade digital descentralizada baseada em blockchain, cuja finalidade é promover a autonomia e controle dos dados pelo usuário. Por fim, analisa dois populares sistemas baseados em blockchain: uPort e sovrin, visando auxiliar projetistas de software interessados na avaliação do mecanismo mais apropriado.*

1. Introdução

Uma identidade digital é um conjunto de informações sobre uma entidade do mundo real (indivíduo, aplicativo ou organização) que permite representá-la e identificá-la em sistemas de informação de forma personalizada. Os sistemas de gerenciamento de identidades (ou DIM, do inglês *Digital Identity Management*) proveem identidades digitais para os usuários e gerenciam autenticação, autorização e compartilhamento de dados. Em um gerenciamento ***centralizado***, há um único provedor de identidades responsável por armazenar os dados da identidade e autenticar os usuários. Os modelos ***federados***, por sua vez, usam serviços de terceiros para armazenar e gerenciar essas informações e otimizar a troca de dados através de relações de confiança nas federações [Wangham and Mello 2010]. Nos ***modelos descentralizados***, os proprietários dos dados podem distribuí-los para terceiros e as organizações podem confiar nas informações do usuário sem serem responsáveis pelos dados nem lidarem com os custos e riscos associados.

Uma das estratégias associadas com identidades descentralizadas é a aplicação da tecnologia de livro razão distribuído (DLT, do inglês *Distributed Ledger Technology*), normalmente baseada em *blockchain*. É um sistema descentralizado de registro de transações que opera de forma segura, estável e sem intermediários, na qual todas as transações são registradas criptograficamente em uma rede distribuída *peer-to-peer* e seus eventos averbados em um livro público de forma inalterável, rastreável e transparente. Tem se apresentado como uma abordagem interessante para o DIM descentralizado.

Por sua vez, o mais recente capítulo na evolução desses sistemas na era da Internet é o conceito de ***identidade autossoberana*** (ou SSI, do inglês *Self-Sovereign Identity*). Segundo [Allen 2016], SSI defende uma forma de identificação dependente apenas do próprio usuário, enraizada em identificadores que não estão sob o controle de uma terceira parte que o ateste, mas que são verdadeiramente controlados pelo indivíduo.

Diante da diversidade de modelos de identificação digital existentes, o objetivo deste artigo é propor uma taxonomia sobre os elementos essenciais de identidade descentralizada e realizar um estudo comparativo dos sistemas: uPort e sovrin, analisando as características que existem em cada um. A contribuição da compilação desses modelos é permitir ao projetista de software avaliar as melhores opções considerando as necessidades e requisitos da aplicação a ser construída ou modificada.

Este artigo está organizado da seguinte forma, a Seção 2 discute os trabalhos relacionados. A Seção 3 detalha a taxonomia proposta. A Seção 4 compara dois sistemas de identidade descentralizada baseadas em *blockchain*. Por fim, a Seção 5 conclui o artigo.

2. Trabalhos Relacionados

Alguns estudos que exploram o estado da arte de sistemas de gerenciamento de identidade descentralizada baseada em *blockchain* podem ser vistos em [Dunphy and Petitcolas 2018] que analisa três sistemas de gerenciamento de identidade na *blockchain* e compara o sovrin, uPort e shoCard em relação às sete leis de identidade de K. Cameron. Em [Elsden et al. 2018] os autores apresentam uma tipologia de aplicativos *blockchain*, incluindo algumas soluções de Gerenciamento de Identidade. No entanto, este estudo não abordou detalhes técnicos das soluções.

O diferencial deste artigo é a proposição de uma taxonomia que compreende os elementos fundamentais de identidade descentralizada baseada em *blockchain* e uma comparação envolvendo as dez características levantadas por [Allen 2016], além de algumas propriedades relacionadas às especificações recentemente padronizadas pela W3C[1].

3. Proposta de Taxonomia sobre os elementos fundamentais de Identidade Digital Descentralizada baseada em Blockchain

Uma taxonomia é, por definição, uma classificação sistemática, utilizada neste artigo como ferramenta de organização intelectual. Na figura 1, fornecemos uma terminologia dos componentes essenciais do sistema de identidades descentralizadas baseadas em *blockchain* visando explicar como funcionam e relacionar com os sistemas sovrin e uPort.

No acesso, realiza-se a vinculação entre uma identidade digital e uma entidade específica, cada um com seus atributos, direitos, autenticação, privilégios de acesso, data

[1]World Wide Web Consortium (W3C) - é a principal entidade de padronização da World Wide Web.

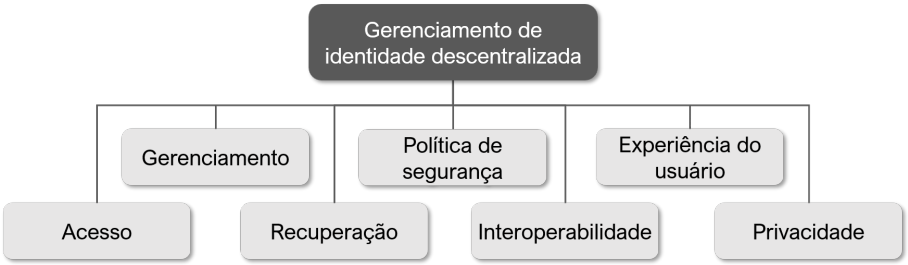

Figura 1. Taxonomia sobre os elementos fundamentais de identidade descentralizada. Fonte: autor

de validade, autorização de uso. Após a autenticação, registros devem ser gerados e, para guardá-los e gerenciá-los, pode-se utilizar protocolos externos, como protocolos de armazenamento descentralizados e retornar os dados ao aplicativo quando forem utilizados [Guy 2019], como o Sistema de arquivos interplanetários (IPFS).

Ao utilizar sistemas de gerenciamento de identidade baseados em DLT, pode-se criar *smart contracts* completos que criam, atualizam ou removem sua identidade, além de gerenciar chaves. O armazenamento das credenciais pode ocorrer na cadeia (*on chain*) ou fora dela (*off chain*). Neste último, as credenciais são armazenadas em um aplicativo de carteira controlada pelo usuário ou armazenadas por um terceiro ao qual o proprietário pode delegar essa função, são os chamados custodiantes. Um identificador descentralizado (DID[2], do inglês Decentralized Identifiers) possui uma camada de operação que se concentra em como executar as funcionalidades CRUD (*Create, Read, Update, Deactivate*) em um documento DID podendo ser usada pelo usuário caso deseje alterar dados.

Para o caso de perda da identidade, deve existir um protocolo de recuperação seguindo mecanismos previamente implementados, como um custodiante designado pelo usuário, uma lista de administradores nomeados etc. Entretanto, tal possibilidade pode apresentar vulnerabilidades, pois os próprios nós de confiança podem se tornar um vetor de ataque, em caso de conluio contra um usuário. Além disso, para um uso eficaz faz-se necessário adotar políticas de segurança, podendo fazer uso de ferramentas de gerenciamento e compartilhamento para evitar o comprometimento de chaves privadas, deve-se compreender a Lei Geral de Proteção de Dados Pessoais (LGPD) e implementar seus pilares, deve-se realizar auditorias e testes e utilizar bibliotecas consolidadas para reduzir a exposição de identificadores por parte de *smart contracts* vulneráveis.

Os sistemas de gerência de identidade devem implementar interfaces compatíveis com padrões internacionais e adotar protocolos padrões, como BIP-32, ERC-20, que possibilitem a criação de carteiras interoperáveis. Pode-se obter interoperabilidade através de Resolvedores Universais, como o resolvedor DID universal, ou através de *Bridges*, que integram recursos de um sistema em outro pela implementação de bibliotecas. Esta taxonomia defende, também, a importância de se priorizar a experiência do usuário, para que não precise saber sobre criptografia, mas entender apenas que seu dispositivo móvel e o aplicativo podem ser usados para interagirem com aplicações descentralizadas (Dapp), fazer login em sites, verificar transações, assinar documentos.

[2]Identificadores Descentralizados (DID) são um tipo de identificador para fornecer identidade digital descentralizada e verificável, independente de terceiros.

Mas o principal requisito a ser considerado é a privacidade, que motiva a adoção de um sistema de gerência de identidade, tentando evitar o uso indevido de informações pessoais. Para preservá-la, o usuário necessita permanecer anônimo, usar pseudônimos (como DID) ou divulgação seletiva - mecanismos que adicionam uma camada de privacidade aos atributos e certificados, criptografando dados e exibindo apenas a informação necessária, uma forma de promover a divulgação seletiva é através de Árvores de Merkle[3] ou de Provas de Conhecimento Zero (ZKP, do inglês *Zero Knowledge Proof*)[4]. As credenciais verificáveis são outra forma de promover a privacidade, pois representam um formato para credenciais digitais interoperáveis e criptograficamente verificáveis que junto com os DID visam erradicar o compartilhamento excessivo de dados.

4. Análise comparativa de Identidades Digitais baseadas em Blockchain

São analisados dois sistemas de gerenciamento de identidades que forneceram detalhes técnicos suficientes sobre suas arquiteturas: **uPort e sovrin**, sendo consideradas suas especificações e documentações.

O uPort [Lundkvist C. and Sena 2016] é um SSI baseado no Ethereum, que é capaz de armazenar *smart contracts*, sua arquitetura consiste em 3 componentes principais: *smart contracts* - que formam o núcleo da identidade, com dois modelos: contrato de controlador e contrato de proxy, cada um incluindo o uPortID -, *aplicativo móvel* - o qual gera um par de chaves assimétricas, mantendo a chave privada no dispositivo, sem possibilidade de exportá-la - e *bibliotecas de desenvolvedores* - que incluem chamadas para suas funcionalidades e integram o uPort aos aplicativos desenvolvidos por terceiros. A Figura 2 apresenta uma visão geral da interação entre um *smart contract* e um Dapp. Para interagir com o contrato de aplicação, o usuário envia para o aplicativo a transação assinada com sua chave, pelo contrato de proxy, através do contrato de controlador.

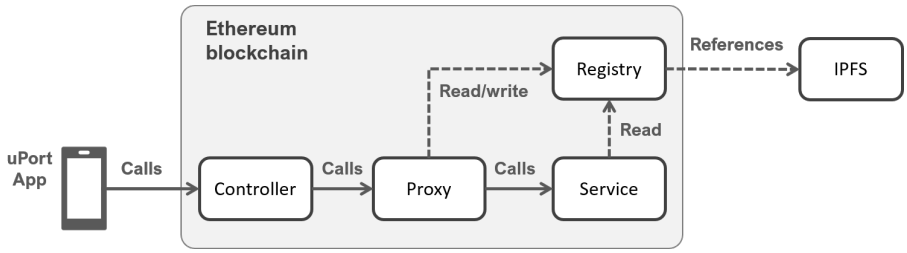

Figura 2. Elementos chave do uPort. Baseado em [Dunphy and Petitcolas 2018]

O sovrin [Tobin and Reed 2017] é um SSI baseado em padrões e código abertos. É público, mas apenas instituições confiáveis (chamadas administradoras ou *stewards*) podem executar nós que participam de protocolos de consenso, sua arquitetura possui três camadas: *Sovrin Ledger* - um livro distribuído de organizações públicas sem fins lucrativos, no qual seus nós executam o protocolo Plenum -, *Agentes Sovrin* - através da qual os usuários interagem com a rede, tornam o cliente endereçável, realizam o armazenamento e compartilhamento de dados criptografados - e *Clientes Sovrin* - que são aplicativos rodando no dispositivo móvel do usuário que comunicam os *agentes* e o *ledger*. Algumas

[3] Árvores de Merkle podem estruturar dados de credenciais, permitindo que os indivíduos, no momento da validação de dados, divulguem apenas partes selecionadas da árvore usando uma prova de Merkle.

[4] As ZKP são esquemas criptográficos nos quais um provador é capaz de convencer um verificador de que uma afirmação é verdadeira sem fornecer mais informações do que o necessário.

funções dos clientes sovrin são gerenciar e proteger as chaves, realizar a autenticação na rede e manter uma cópia local do contêiner de dados sovrin do proprietário.

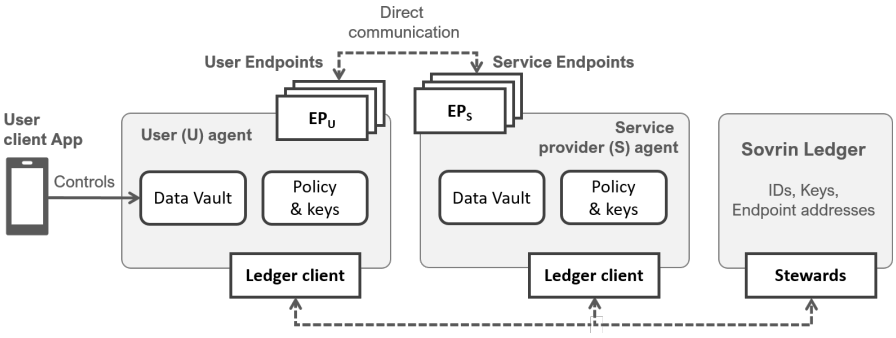

Figura 3. Elementos principais do sistema sovrin [Dunphy and Petitcolas 2018]

As propriedades definidas abaixo e compiladas na Tabela 1 foram utilizadas para formar a base do comparativo entre sovrin e uPort, relacionando os elementos identificados na taxonomia com a visão definida por [Allen 2016] que levanta um conjunto de recursos agrupados em três categorias: segurança, controlabilidade e portabilidade.

Como descrito na taxonomia, deve existir um aplicativo no dispositivo móvel dos usuários, o que ocorre no uPort e no sovrin. Eles contêm os dados vinculados à identidade e às chaves privadas, usadas para assinatura digital. Facilitando o *acesso* e *controle* por parte dos usuários, que dão seu *consentimento* antes que suas informações sejam utilizadas. Através desses aplicativos, pode-se criar uma identidade sem a intervenção de terceiros e ter *existência* independente. Recomenda-se criar vários identificadores adequando-os a cada contexto no qual seja necessário para manter a privacidade. Para auxiliar com os muitos ID, o sovrin mantém um registro de mapeamento de chaves e identificadores. O uPort também permite criar e divulgar uPortIDs específicos, gerando um novo par de chaves assimétricas e enviando uma transação para a Ethereum que gera uma instância de um controlador com uma referência para cada nova chave pública.

Os sistemas analisados promovem a SSI e permitem ao usuário controlar sua identidade, gerenciar credenciais e criar registros criptograficamente verificáveis. Sugere-se que a comunicação ocorra usando os padrões do W3C, proporcionando *interoperabilidade*. O sovrin e o uPort utilizam credenciais verificáveis com DID, para troca interoperável de credenciais. O uPort utiliza Credenciais Verificáveis nas credencias JWT.

Outra propriedade é a *transparência*, ambas as abordagens são baseadas em padrões e em bibliotecas de código aberto. O sovrin utiliza código-fonte aberto revisado por pares, como o Plenum, que gerencia como chegar a um consenso no razão. Também atendeu a característica da *persistência*, que define que a identidade só deve ser removida e atualizada pelo usuário. O uPort e o sovrin guardam a chave privada localmente e o hash da identificação nas DLTs. Para evitar a perda da identidade, adotam um sistema de administradores, definidos previamente, permitindo a recuperação de uma identidade. As blockchain Ethereum são *permissionless* e a Hyperledger é *permissioned*. Aquela permite que qualquer pessoa na rede opere um nó que participa do consenso. Nesta, embora a blockchain seja pública, apenas os nós administradores podem participar do consenso, o sovrin foi assim projetado para não ter que realizar cálculos caros para chegar ao consenso, diminuindo custos com energia, aprimorando a perfomance e o tempo de resposta.

As informações sobre identidade devem atender ao quesito da *portabilidade*, uPort utiliza o formato JSON e o sovrin usa JSON-LD. Com relação à *privacidade*, o sovrin utiliza protocolo de consenso ZKP que permite a divulgação seletiva de reivindicações. O uPort gera tokens JWT para as verificações e para fornecer *minimização* dos dados. Quanto ao direito de *proteção*, o sovrin garante essa característica pelos nós administradores da rede. O uPort possui *smart contracts* a serem seguidos e os delegados que atestam as identidades dos usuários. No que tange a *experiência do usuário* e, conforme demonstrado na taxonomia proposta, deve-se tornar os sistemas mais intuitivos e menos complexos, propriedade adotada pelo uPort utilizando QR code para iniciar interações.

Tabela 1. Tabela de Comparação de requisitos dos sistemas SSI: uPort e Sovrin.

Características	uPort	Sovrin
Controlabilidade, segurança, portabilidade e recuperação de chave	✓	✓
Blockchain permissionless	✓	–
Blockchain permissioned	–	✓
Experiência do usuário	✓	–
Experiência entre contexto por QR code	✓	–
Uso de Credenciais Verificáveis contendo uma CredentialSchema	–	✓
Uso de Credenciais Verificáveis dentro de credencias JWT	✓	–

5. Conclusão

Este trabalho fornece uma compreensão dos benefícios, desafios e oportunidades dos sistemas de identidades descentralizadas baseados em DLT. Discute os componentes desses tipos de sistemas e identifica os padrões emergentes e suas propriedades. Evidencia o potencial desses sistemas para propiciar aos usuários o controle de seus identificadores e credenciais. Propõe uma taxonomia com os elementos essenciais de um sistema de identidade descentralizada baseada em *blockchain*, que foi utilizada para realizar uma análise comparativa do que é abordado pelos sistemas sovrin e uPort, abordando entre estas características especificações padronizadas pelo W3C, como as credenciais verificáveis.

Referências

Allen, C. (2016). The Path to Self-Sovereign Identity. Acessado em novembro de 2019.

Dunphy, P. and Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security Privacy*, 16(4):20–29.

Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C., and Vines, J. (2018). Making sense of blockchain applications: A typology for hci. New York, USA.

Guy, A. (2019). Encrypted Data Vaults. Rebooting the Web of Trust IX. Acessado em fevereiro de 2020.

Lundkvist C., Heck R., J. T. Z. M. and Sena, M. (2016). UPORT: A Plataform for Self-Sovereign Identity. Acessado em dezembro de 2019.

Tobin, A. and Reed, D. (2017). The Inevitable Rise of Self-Sovereign Identity. Acessado em dezembro de 2019.

Wangham, M. and Mello, E. R. (2010). Gerenciamento de Identidades Federadas. Acessado em janeiro de 2020.