Sobre o uso de Blockchain em soluções com Credenciais Verificáveis e Identidades Auto-Soberanas

Marcus R. Xavier[1,2], Kalil Cabral[2], Ioram S. Sette[2], Carlos A. G. Ferraz[1]

[1] Centro de Informática – Universidade Federal de Pernambuco (UFPE)
{mrxl, cagf}@cin.ufpe.br

[2]Centro de Estudos e Sistemas Avançados do Recife (CESAR)
{kbcv, iss}@cesar.school

Resumo. *Identidade Auto-Soberana - Self-Sovereign Identity (SSI) é um novo modelo que coloca o usuário em posição central em relação à gestão e ao uso de suas identidades. Este modelo vem chamando atenção da academia e da indústria e vem se tornando realidade através de Credencial Verificável - Verifiable Credential (VC) que foi elaborado pela World Wide Web Consortium (W3C). Como resultado preliminar de uma revisão da literatura sobre SSI e VCs, percebeu-se que a maioria das implementações do componente Registro de Dados Verificáveis - Verifiable Data Registry (VDR), responsável por estabelecer uma relação de confiança entre emissores e verificadores de credenciais, utiliza a tecnologia de blockchain. O propósito deste trabalho é iniciar uma discussão sobre o uso de blockchains para a implementação do VDR.*

1. Introdução

A gestão de identidade está passando por uma transição de modelos: das Federações de Identidade, em que os Provedores de Identidade - *Identity Providers* (IdPs) controlam as informações dos usuários, para as Identidades Auto-Soberanas - *Self-Sovereign Identities* (SSIs), em que os usuários estão no centro e gerenciam seus dados, podendo proteger a privacidade dos mesmos. Em todos os modelos precursores de SSI, os dados sempre foram armazenados e gerenciados por terceiros, nunca pelos usuários, seus verdadeiros donos. Os IdPs têm a possibilidade de rastrear que serviços seus usuários utilizam, quebrando a privacidade dos mesmos [Laborde et al. 2020], indo na contramão de regulamentações como a Lei Geral de Proteção de Dados Pessoais (LGPD). Portanto, o novo modelo traz uma quebra de paradigma, pois oferece controle dos dados aos usuários, permitindo que eles acessem diretamente serviços sem intermédio de IdPs [Naik and Jenkins 2020].

Para tornar o modelo de SSI realidade, a especificação de Credenciais Verificáveis - *Verifiable Credentials* (VCs) foi elaborada. O Registro de Dados Verificáveis - *Verifiable Data Registry* (VDR) é a entidade mais controversa quanto à sua implementação. Embora a especificação seja não normativa quanto à tecnologia usada para implementação, é recorrente o uso de registros distribuídos através da tecnologia de *blockchain* [Sporny et al. 2019]. Sendo assim, o objetivo deste trabalho é apresentar vantagens e desvantagens deste uso envolvendo *blockchain*.

Este trabalho está organizado da seguinte forma: na seção 2 são apresentados resultados preliminares de uma revisão sistemática que está sendo conduzida e que serviu

como base para a discussão realizada neste trabalho. A discussão sobre o uso de *blockchain* na camada de VDR é feita na seção 3. Por fim, na seção 4 são apresentadas as conclusões do trabalho.

2. Revisão da Literatura

Uma revisão da literatura com o objetivo de responder a pergunta "Qual o estado da arte das Identidades Auto-Soberanas?" está sendo realizada com base na proposta de [Kitchenham and Charters 2007], que consiste de diversas fases. As quatro bibliotecas digitais mais populares na área de ciência da computação foram utilizadas na condução da pesquisa: ACM, IEEE, Science Direct e Springer.

Inicialmente, utilizou-se uma *string* de busca englobando tanto o modelo Identidade Auto-Soberana - *Self-Sovereign Identity* (SSI) quanto o padrão Credencial Verificável - *Verifiable Credential* (VC). Caso uma busca mais especializada fosse necessária, essa poderá ser feita posteriormente usando os resultados obtidos como entrada para a condução de uma nova revisão mais profunda em um tópico de interesse. Após algumas etapas de calibração a *string* definida foi *"Self-Sovereign Identity" OR "Verifiable Credentials"*.

Como resultado das buscas, foram encontrados um total de 220 trabalhos, sendo 31 na ACM, 64 na IEEE, 48 na Science Direct e 77 na Springer, sendo 17 artigos de revistas e 60 artigos de conferência. Em seguida os resultados foram tabulados para avaliação dos títulos e resumos. Após esta fase, do total de 220 trabalhos avaliados, 84 foram classificados como de fato relacionados com a pesquisa.

Na fase de avaliação da qualidade dos trabalhos foram definidos 7 atributos de qualidade sobre SSI: a Motivação para sua Criação; Vantagens e Desvantagens; Exemplos de Uso; Se Apresenta Padronizações; Desafios Atuais; Forma de Avaliação; e Tecnologias. Para cada um dos atributos foram atribuídas uma das notas: 0 (zero) para quando a pergunta não fosse respondida pelo trabalho; 0,5 quando fosse respondida parcialmente; e a nota 1 quando a pergunta fosse respondida claramente. Ao final foi calculada uma média simples considerando as notas obtidas por cada trabalho, chegando-se a 29 artigos com média maior ou igual a 0,7, considerada a nota de corte.

Como resultado geral da revisão da literatura conduzida até o momento, confirmamos o uso dominante de *blockchain* em VCs, preliminarmente na ordem de 97%. Cabe ressaltar que, devido à limitação de espaço, as respostas propriamente ditas aos sete atributos de qualidade da revisão estão fora do escopo deste artigo.

3. Uso de Blockchain em VCs

A camada de Registro de Dados Verificáveis - *Verifiable Data Registry* (VDR), presente na especificação da World Wide Web Consortium (W3C) para Credenciais Verificáveis - *Verifiable Credentials* (VCs), possui diversas finalidades, dentre as quais destacam-se o estabelecimento de relações de confiança entre as entidades e a divulgação de esquemas que definem as propriedades contidas nas VCs. A relação de confiança entre emissores (*issuers*) e portadores (*holders*) é importante para que as credenciais sejam emitidas para quem tem direito de gerenciá-las e sejam guardadas com segurança e confidencialidade. Os verificadores (*verifiers*) devem confiar em um conjunto de *issuers* para emitir determinados tipos de credenciais, como, por exemplo, confiar apenas no Departamento de

Trânsito para emissão de carteiras de motorista. Por fim, em muitas ocasiões, o Provedor de Serviço - *Service Provider* (SP) também precisa identificar os *holders* das credenciais para prover o serviço de forma personalizada.

Uma forma bastante utilizada para estabelecer relações de confiança entre as entidades é através da troca de chaves criptográficas. Embora a especificação da W3C não seja restritiva quanto aos mecanismos para o estabelecimento de provas de autenticidade das VCs, esta é restritiva quanto à existência de algum mecanismo de comprovação e quanto à localização das informações necessárias para a verificação destas provas [Sporny et al. 2019]. Atualmente, estão mapeados pelo W3C *Credentials Community Group* dois mecanismos de comprovação, isto é, assinaturas RSA e assinaturas Ed25519 [Credentials Community Group 2020], ambos algoritmos de criptografia assimétrica amplamente utilizados na indústria. Para a verificação da assinatura, se faz necessária a recuperação de uma chave pública associada à entidade assinante e, uma vez recuperada, é possível estabelecer confiança na autenticidade e integridade da credencial.

Nas implementações de Identidade Auto-Soberana - *Self-Sovereign Identity* (SSI) que utilizam *blockchain*, as entidades publicam suas chaves públicas num registro distribuído e, através desse processo, obtém um identificador, o Identificador Descentralizado - *Distributed IDentifiers* (DID). Quando uma entidade precisa verificar a autenticidade dos emissores, *issuers* no caso de VCs e *holders* no caso de Apresentações Verificáveis - *Verifiable Presentations* (VPs), o DID pode ser utilizado para recuperar tais chaves. Um exemplo disso é durante a etapa de verificação das credenciais pelo *verifier*. Esse mecanismo pode ser observado em diversas implementações de VCs, como Sovrin e uPort [Bernal Bernabe et al. 2019, Tobin 2018, Lundkvist et al. 2016].

Quando o DID se refere ao emissor, armazená-lo em locais públicos como as *blockchains* é necessário, uma vez que outras entidades, como os portadores e verificadores, podem facilmente obtê-las e garantir que estão se comunicando com a entidade na qual confiam. Nesse contexto, o VDR atua como um repositório confiável de chaves públicas. No entanto, como alternativa a *blockchains*, o VDR pode ser implementado por um banco de dados centralizado ou qualquer outra forma de distribuição e/ou resolução de chaves públicas.

Quando a comunicação envolve o portador, os mecanismos não deveriam expor sua identidade, como forma de garantir sua privacidade. Nestes casos, o uso de *blockchains* é desaconselhável. Por este motivo, muitas implementações utilizam identificadores *off-ledger*, ou seja, fora da *blockchain*, para gerenciar DIDs e VCs. Apesar disto, encontramos algumas implementações de VCs, como a ShoCard, que utilizam a *blockchain* para o registro e identificação das credenciais em si.

[Chadwick et al. 2019] propõe uma implementação de VCs sem o uso de *blockchains*. Nela, o protocolo Universal Authentication Framework (UAF) do Fast IDentity Online (FIDO) é usado para estabelecer uma relação de confiança entre portadores e emissores. No entanto, a relação de confiança entre emissores e verificadores é deixada em aberto.

Há ainda outras formas de uso de *blockchains* relacionado a SSI. Quanto a gestão de esquemas que definem os formatos e propriedades das VCs, o uso de uma blockchain não é necessário, pois existem outras formas de distribuir esquemas entre entidades

num ecossistema. *Blockchains* também são usadas para o controle de um registro de revogações, em conjunto com uma tecnologia de *Zero-knowledge Proof*, sem divulgar qualquer detalhe da credencial em si. Mais uma vez, como alternativa, pode-se olhar para outras soluções existentes na indústria para gestão de revogações, que vão desde bancos de dados centralizados até a redução no tempo de vida dos certificados.

4. Conclusão

Como discutido neste trabalho, o uso de *blockchain* na implementação de SSI e VC é muito frequente, ainda que na especificação da W3C não seja sugerido o uso desta tecnologia. Compreendemos a origem deste fato a partir da concepção dos DIDs, porém já não recomenda-se que sejam publicados em bases públicas na maioria dos casos por motivos de privacidade. Portanto, é natural questionar o por quê desta preferência por *blockchain*, dadas desvantagens como, por exemplo, o alto consumo energético no caso de *Proof of Work*, o tempo que leva para adicionar informações ou a imutabilidade que pode colocar a privacidade e a reputação dos usuários em risco [Gatteschi et al. 2018]. A análise aprofundada de algumas destas desvantagens e a busca de alternativas abrem espaço para trabalhos futuros.

Referências

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., and Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, 7:164908–164940.

Chadwick, D. W., Laborde, R., Oglaza, A., Venant, R., Wazan, S., and Nijjar, M. (2019). Improved Identity Management with Verifiable Credentials and FIDO. *IEEE Communications Standards Magazine*, 3(4):14–20.

Credentials Community Group (2020). Verifiable Credentials Extension Registry. Technical report, W3C.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., and Santamaría, V. (2018). To blockchain or not to blockchain: That is the question. *IT Professional*, 20(2):62–74.

Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering.

Laborde, R., Oglaza, A., Wazan, S., Barrere, F., Benzekri, A., Chadwick, D. W., and Venant, R. (2020). A User-Centric Identity Management Framework based on the W3C Verifiable Credentials and the FIDO Universal Authentication Framework. *IEEE CCNC 2020*.

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., and Sena, M. (2016). UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY. Technical report.

Naik, N. and Jenkins, P. (2020). Self-Sovereign Identity Specifications: Govern Your Identity through Your Digital Wallet using Blockchain Technology. *Proceedings - IEEE MobileCloud 2020*, (Idm):90–95.

Sporny, M., Longley, D., and Chadwick, D. (2019). Verifiable credentials data model 1.0. `https://www.w3.org/TR/vc-data-model/`. [Online; accessed 23-August-2021].

Tobin, A. (2018). Sovrin: What Goes on the Ledger? Technical report, Evernym.