Modelo de gerência utilizando identidade autossoberana para transporte: Caso de uso voltado ao ecossistema de um condomínio de empresas

Bruno Evaristo, Ismael Ávila, Jeffson Celeiro

[1]Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

{elderb,avila_an,jcsousa@cpqd.com.br

Abstract. *This paper discusses the use of decentralized digital identities as credentials for access to public transportation. The practical case that inspired the study is the identification of users of a bus service that serves a technology park in Campinas, Brazil, a context that has similarities with the public transportation. The paper proposes a model for user management through the issuance of verifiable and standardized transportation credentials. In this first stage of the study, the advantages and challenges of the solution are discussed and some requirements are elicited from stakeholders.*

Resumo. *Este trabalho discute o uso de identidades digitais descentralizadas como credenciais de acesso ao transporte coletivo. O caso prático que inspirou o estudo é o da identificação dos usuários de um serviço de ônibus que atendem a um condomínio de empresas em Campinas, contexto que tem semelhanças com o transporte público. O trabalho propõe um modelo de gerência dos usuários por meio da emissão de credenciais de transporte verificáveis e padronizadas. Nesta primeira etapa do estudo, são discutidos as vantagens e os desafios da solução e levantados alguns requisitos com partes interessadas.*

1. Introdução

O cenário atual do transporte público é muito fragmentado e despadronizado em razão da variedade de soluções, modelos e formatos de gestão da demanda, de precificação e de tratamentos dos dados. Alguns sistemas oferecem soluções integradas para diferentes modais de transporte, como é o caso da cidade de Curitiba, enquanto outros operam de maneira menos integrada. Por outro lado, as soluções de gerenciamento existentes variam da emissão de bilhetes em papel ao uso de cartões inteligentes. Um dos principais desafios dessa fragmentação é o gerenciamento de contas de usuários em sistemas de transporte público independentes [Alyavina et al. 2022].

No que se refere à confidencialidade dos dados pessoais, a conectividade dos sistemas à internet representa um risco. No entanto, a integridade e a privacidade dos dados na internet pode ser assegurada por tecnologias tais como a blockchain. Esta, além disso, propicia elevada transparência, algo essencial quando se lida com várias partes interessadas, como os diferentes atores envolvidos em um serviço de transporte. Mas tudo isso requer um sistema de gestão de contas que permita aos usuários uma total autonomia no acesso e na gestão de seus dados. Em geral, sistemas de gestão de identidade são hospedados em bancos de dados centralizados que são controlados e geridos pelos prestadores

do serviço. No entanto, organizações como o World Wide Web Consortium (W3C) trabalham em novos conceitos e padrões para soluções de identidade digital descentralizada (IDD) [Brooks 2017]. Assim, este trabalho investiga o uso de IDDs interoperáveis como credenciais de acesso ao transporte coletivo, seja ele público ou privado.

O estudo foi motivado por um caso prático de identificação dos usuários de um serviço de ônibus que atende a um condomínio de empresas em Campinas. O serviço tem natureza multiponto-ponto nos trajetos de ida e de ponto-multiponto nos trajetos de volta. Isso significa que, sem uma solução eficaz de identificação digital, um controle mais criterioso dos embarques só é viável nas dependências do condomínio, antes das viagens de retorno, quando os motoristas conseguem inspecionar visualmente o crachá de cada passageiro para verificar se este trabalha em uma das empresas contratantes do serviço e é cadastrado naquela linha. Isso permite restringir o uso do serviço por pessoas não cadastradas e, no caso de linhas muito concorridas, priorizar os usuários cadastrados nelas. Todavia, além de não gerar registros digitalizados do perfil de uso do serviço, de modo a facilitar sua gestão, a inspeção visual dos crachás é dificultada pelo fato de se utilizarem do serviço cerca de dez empresas do condomínio, o que exige dos motoristas memorizar diversos leiautes de crachá, os quais, de resto, podem sofrer remodelagens periódicas. E as inspeções visuais são ainda menos efetivas nos acessos feitos nos vários pontos de embarque ao longo dos trajetos de ida até o condomínio, e o uso indevido já provocou situações de superlotação, com significativos transtornos.

Nesse sentido, esse caso prático tem semelhanças com o transporte público, com diversos pontos de embarque e desembarque em vias públicas, ao longo dos vários itinerários atendidos. Assim, o trabalho propõe um modelo de gestão dos usuários por meio da emissão de credenciais de transporte verificáveis e padronizadas. Na primeira etapa, estão sendo estudadas as vantagens e os desafios da solução e levantados requisitos junto a partes interessadas. Nas etapas subsequentes, é previsto um piloto da solução, de modo a avaliar seus ganhos e seu potencial para ser aplicada, de forma mais ampla e interoperável, ao serviço público de transporte.

O restante do artigo está assim organizado: A Seção 2 apresenta o referencial teórico. A Seção 3 explica como o ecossistema está estruturado. A Seção 4 demonstra o caso de uso teórico baseado no ecossistema, e a Seção 5 apresenta a conclusão e trabalhos futuros.

2. Referencial Teórico

Nesta seção, os fundamentos dos tipos e gerenciamento de identidade são revisados e, em seguida, discute-se como a tecnologia blockchain pode ser útil na gestão das identidades dos usuários de um serviço.

2.1. Gerenciamento de identidade digital descentralizada

Os sistemas de gestão de identidade digital descentralizada (IDD) em geral compreendem três papéis principais: o provedor ou emissor da identidade, o proprietário ou titular da identidade e o provedor de um serviço acessado por meio da identidade. A relação entre esses três papéis define um triângulo da confiança, como ilustrado na Figura 1.

Os proprietários de identidade podem receber credenciais de diferentes emissores e serviços e a carteira digital que armazena essas credenciais pode também conter mais

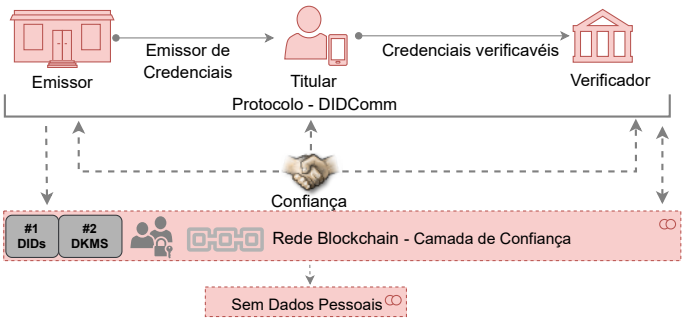

Figura 1. Triângulo da confiança de SSI

informações pessoais do proprietário [Soltani et al. 2021]. O proprietário da identidade pode apresentar ao provedor de um serviço, como prova, todo o seu conjunto de credenciais ou parte delas, em combinações variadas.

2.2. Blockchain no gerenciamento de identidade

Redes de gerenciamento de IDD utilizam a tecnologia blockchain para eliminar a necessidade de provedores de identidade intermediários. Assim, no contexto das chamadas *identidades autossoberanas* (SSI), a blockchain é uma tecnologia-chave para assegurar aos usuários o pleno controle sobre suas identidades. Neste caso, as identidades estão vinculadas aos chamados identificadores descentralizados (DIDs), criados e armazenados em blockchains. Esses identificadores podem ser vinculados a determinados documentos e credenciais, que os usuários podem controlar de forma autônoma. Além disso, a interoperabilidade entre os sistemas pode ser garantida, uma vez que os usuários não ficam presos a um provedor de identidade específico que não queira integrar-se a serviços fora de seu próprio ecossistema.

3. Exemplo de ecossistema de identidade digital descentralizada

A Figura 2 representa a SOUiD[1], uma iniciativa da Fundação CPQD de criação de um ecossistema de identificação digital [de Souza et al. 2022]. Nele, a instituição é responsável pela emissão das credenciais de identidade de seus colaboradores (usuários da solução). O processo de registro de um novo usuário pode envolver biometria, verificação de documentos, comparecimento presencial, etc. O nível de segurança é definido, portanto, pelo emissor. Uma vez registrado um novo usuário, o emissor cria uma credencial digital que pode ser armazenada com uma chave criptográfica na aplicação SOUiD e pode ser utilizada pelos colaboradores no acesso a serviços corporativos por meio de credenciais seguras. Um possível uso, atualmente em discussão, seria no controle de acesso ao serviço de ônibus fretados que transporta os colaboradores da fundação. Todavia, como o serviço atende a várias empresas instaladas no mesmo condomínio corporativo, a aplicação SOUiD precisaria ser adotada por todas elas, de forma consorciada, e reconhecida pelos gestores do serviço. Para tanto, e com vistas a uma futura prova de conceito (PoC) da aplicação, foram levantados junto a esses gestores os principais requisitos da gestão desse serviço, conforme discutidos a seguir.

[1] https://www.cpqd.com.br/solucoes/id/

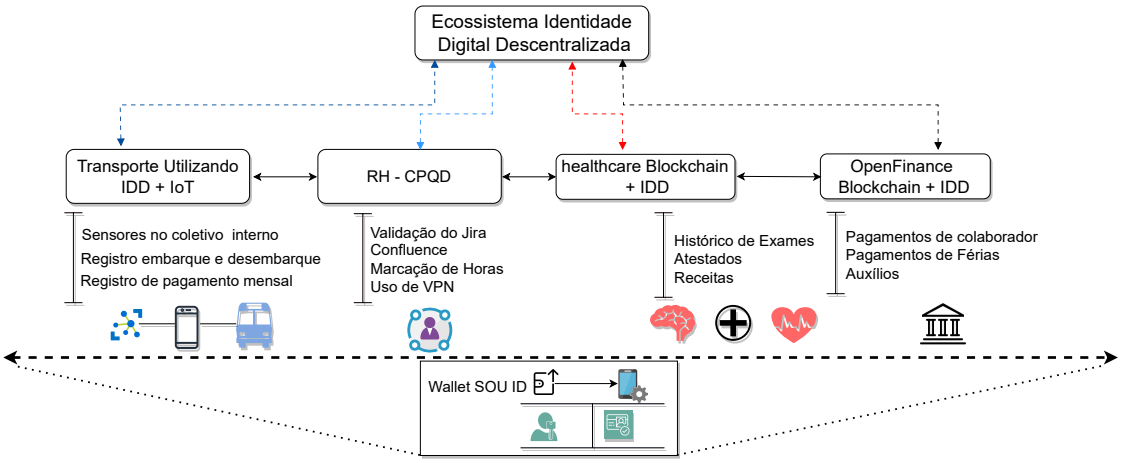

Figura 2. Ecossistema de identidade digital descentralizada

3.1. Modelo de Gerência

Com base nos princípios de SSI, esta seção enfoca a identificação dos requisitos gestão de identidade descentralizada no serviço de transporte que atende ao condomínio. Conceitos tais como identificadores descentralizados, esquemas, credenciais e o processo geral de verificação de identidade são extraídos de implementações atuais de sistemas de gestão de identidade, bem como requisitos que podem ser derivados de interações e relacionamentos específicos entre diferentes partes interessadas no setor de transporte. No levantamento de requisitos junto aos gestores do condomínio, constatou-se que já foram tentadas ou cogitadas algumas alternativas, sem que tenha sido encontrada uma solução satisfatória. Assim, por exemplo:

- O uso de etiquetas com código QR na entrada dos ônibus causou lentidão, pois ao embarcar cada passageiro deveria usar seu *smartphone* fazer o *checkin*. Para atenuar o problema, as etiquetas foram também afixadas à frente de cada assento. Todavia, nesse caso não havia como o motorista controlar se todos de fato faziam o *checkin*. Consequentemente, os dados de embarque não eram confiáveis e não possibilitavam uma gestão precisa da demanda. E essa falta de previsibilidade tornou-se ainda maior com a adoção de regime de trabalho semipresencial por várias empresas do condomínio;
- O uso dos identificadores por radiofrequência (RFID), já existentes nos crachás, traria como dificuldades a etapa de cadastramento físico do crachá de cada usuário do transporte e também o prazo de confecção do crachá de cada novo colaborador, sendo comum entre as empresas o uso de crachás provisórios, sem RFID;
- O uso de um *app* do serviço com funcionalidade de *checkin* já é previsto no *road-map* da empresa prestadora e poderia integrar a SOUiD. Todavia, por questões de segurança relacionadas à funcionalidade de geolocalização dos veículos, o acesso ao *app* somente deveria ser permitido a usuários cadastrados. Assim, na visão dos gestores, além do controle do acesso aos veículos a IDD poderia controlar o acesso ao próprio *app*;
- Por fim, como o condomínio corporativo reúne empresas de tecnologia, os gestores consideram que uma solução inovadora, como o uso de IDDs e carteiras digitais, traria um claro ganho de imagem para o empreendimento.

4. Casos de Uso

- **Caso de Uso 1: Solicitação de credencial de transporte**

O caso prático trata da identificação dos usuários do serviço de ônibus do condomínio, que é prestado mediante cadastramento prévio dos passageiros, colaboradores das várias empresas ali situadas. Todavia, ao longo dos anos o acesso ao serviço esteve sujeito ao uso indevido por passageiros não cadastrados, em razão das dificuldades relatadas no levantamento de requisitos. Diante disso, no que trata da solução proposta, na solicitação de credencial de transporte, assim que um colaborador tiver reunido todas as informações exigidas, ele deve entrar em contato com os gestores do serviço. Se todos os documentos apresentados forem válidos, ele recebe uma credencial para usar o serviço. Conforme mostrado na Figura 3, o solicitante e o provedor de identidade (neste caso, a autoridade de transporte) estabelecem uma relação de confiança. O colaborador apresenta um conjunto de informações necessárias para a emissão da credencial de transporte.

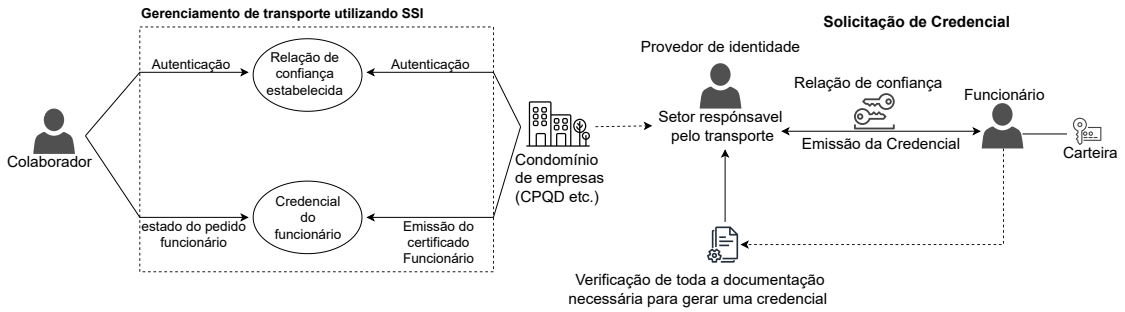

Figura 3. Solicitação de credencial de transporte

Por meio de provas criptográficas, o emissor valida a exatidão das declarações fornecidas. Feita essa validação, a credencial de viagem é emitida e se torna um documento digital oficial, como qualquer outra credencial verificável. Por fim, o colaborador armazena a credencial para uso futuro em sua carteira digital ou Identity Hub.

- **Caso de Uso 2: Uso da credencial**

O fluxo do caso de uso descreve o processo que ocorre quando o colaborador usa sua credencial. Após estabelecida a relação de confiança, a comprovação precisa ser apresentada pelo colaborador por meio de sua carteira digital (*wallet*). Ao obter com êxito a credencial de viagem e incluí-la na carteira digital em seu celular, o colaborador passa a poder utilizar o serviço imediatamente, sem a necessidade de confecção de um *token* físico (como os crachás com RFID). Os embarques e desembarques passam a ser registrados automaticamente por um sensor de proximidade junto à porta do veículo, que verifica na rede blockchain a validade da credencial. Caso o passageiro não tenha credencial, um alerta é emitido. O mesmo ocorre caso ele acesse uma linha em que não esteja cadastrado, e a solução verifique no histórico que há risco de *overbook*. As informações podem ser tratadas como uma credencial da transação, bem como um recibo de uma viagem, contendo localização e hora do *check-in* e do *check-out*, como ilustrado na Figura 4.

Após validar o comprovante emitido pelo prestador, o gestor do serviço pode dar acesso ao sistema, que trata o serviço como uma credencial que pode ser usada como

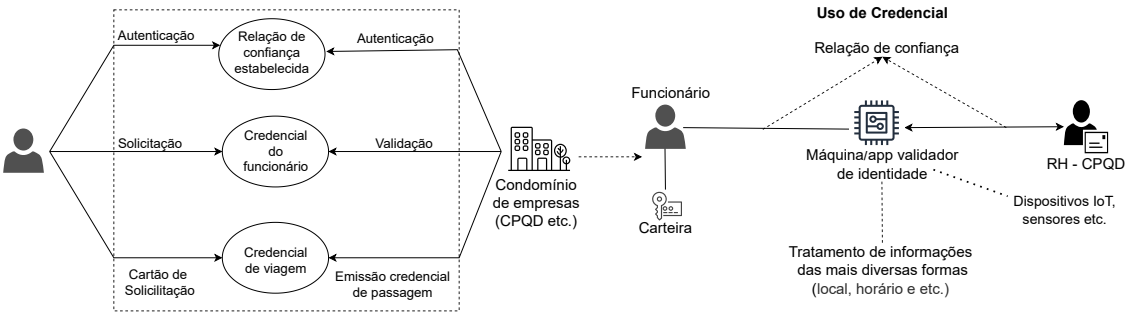

Figura 4. Uso da credencial no ecossistema

recibo de uma viagem para provar a qualquer outra pessoa que um determinado *check-in* ou *check-out* ocorreu. Além disso, o sistema pode interagir com soluções *off-chain* para acionar eventos adicionais (por exemplo, uma solicitação de cobrança).

5. Conclusão e trabalhos futuros

Com base nos princípios das SSI, neste artigo foi proposto um modelo de gestão de identidade descentralizada, exemplificado em um cenário básico no qual os usuários, colaboradores de empresas de um condomínio corporativo, têm acesso a um serviço de ônibus por meio de credenciais emitidas pelos gestores e verificadas pelos prestadores do serviço. Esse caso de uso tem bom potencial de validação prática num piloto da aplicação SOUiD como prova de conceito. E, dada a semelhança com o transporte coletivo público, possibilita avaliar a expansão da solução para atender esse serviço.

Como trabalhos futuros, é prevista uma prototipagem do modelo, com vistas a aplicar a solução ao referido serviço de transporte, uma situação real, mas em ambiente controlado. Isso permitirá avaliar sua futura aplicação no transporte público, de modo a propiciar a seus usuários uma forma mais segura, padronizada e interoperável de identificação por meio de SSI. Com isso, a solução possibilitaria propor e testar formas de pagamento aberto, ou as DeFis, nas quais se pode, a partir de uma carteira, vincular uma credencial válida a outras formas ou sistemas de gestão, seja financeira, seja de demanda, entre outras, dentro de um ecossistema interoperável.

Referências

[Alyavina et al. 2022] Alyavina, E., Nikitas, A., and Njoya, E. T. (2022). Mobility as a service (maas): A thematic map of challenges and opportunities. *Research in Transportation Business & Management*, 43:100783.

[Brooks 2017] Brooks, T. (2017). World wide web consortium (w3c). In *Encyclopedia of Library and Information Sciences*, pages 5034–5038. CRC Press.

[de Souza et al. 2022] de Souza, F., Formigoni Filho, J. R., Marino, F. C. H., and Sampaio, A. S. (2022). Autenticaçao segura de pessoas com carteira digital: um estudo no cpqd. In *Anais Estendidos do XXI Simpósio Brasileiro de Fatores Humanos em Sistemas Computacionais*, pages 48–55. SBC.

[Soltani et al. 2021] Soltani, R., Nguyen, U. T., and An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, 2021:1–26.