Gerenciamento Descentralizado de Identidades para Cidades Inteligentes usando Neo Blockchain

Valesca Moura de Sousa[1]

[1]Instituto de Computação – Universidade Federal Fluminense

valescamoura@id.uff.br

Abstract. *Smart cities are cities that use technology to make the environment more sustainable and efficient. Governments can make decisions based on data collected by sensors and IoT devices. Therefore, the veracity and security of the data is essential and the use of digital identities to verify permissions is a resource used for this purpose. In this work, a model for decentralized identity management based on Neo Blockchain, specifically aimed at the context of smart cities, will be presented. This work is a simplified implementation of the solution proposed in the article Gerenciamento Descentralizado de Identidades para Cidades Inteligentes Baseado na Tecnologia Blockchain published in SBSeg 2022 [Cardoso et al. 2022].*

Resumo. *Cidades inteligentes são cidades que utilizam a tecnologia para tornar o ambiente mais sustentável e eficiente. Órgãos públicos podem tomar decisões com base em dados coletados por sensores e dispositivos IoT. Por isso, a veracidade e segurança dos dados é imprescindível e o uso de identidades digitais para verificar permissões é um recurso utilizado para este fim. Neste trabalho será apresentado um modelo para gestão descentralizada de identidades baseado na Neo Blockchain, especificamente voltado para o contexto das cidades inteligentes. Este trabalho é uma implementação simplificada da solução proposta no artigo Gerenciamento Descentralizado de Identidades para Cidades Inteligentes Baseado na Tecnologia Blockchain publicado na SBSeg 2022 [Cardoso et al. 2022].*

1. Introdução

Cidade Inteligente (CI) e o termo utilizado para representar o conceito de redução dos problemas causados pela urbanização por meio da utilização de novas tecnologias, tornando o ambiente da cidade mais sustentável e eficiente [Xie et al. 2019]. Nestas cidades, o uso de dispositivos inteligentes são amplamente utilizados para diversos fins, inclusive para tomada de decisões de órgãos públicos. Economia na iluminação pública através de sensores, gerenciamento do trânsito, acompanhamento em tempo real de ambulâncias e caminhões de bombeiros, e detecção do nível de resíduos de lixeiras para notificação das equipes de coleta são exemplos disso. A Internet das Coisas (*Internet of Things*, IoT) é, portanto, uma tecnologia importante na construção de cidades inteligentes.

A cibersegurança é uma das mais importantes preocupações no contexto de cidades inteligentes pois é vital que os dados e a infraestrutura da cidade estejam seguros contra ataques cibernéticos [Alamer and Almaiah 2021], como acesso não autorizado a

serviços e dados. Dados coletados por sensores devem manter sua integridade e privacidade, assim como é fundamental verificar a identidade dos dispositivos que acessam os sistemas da CI: ”Em um ambiente de uma Cidade Inteligente, onde podem existir milhões de dispositivos IoT consumindo e produzindo dados, a gestão de identidades se apresenta como forma de aprimorar o ambiente da cidade em relação á segurança computacional. Dados produzidos por dispositivos em uma CI são utilizados para tomar decisões ou atuar sobre o ambiente da cidade, e isto se reflete diretamente nos recursos da cidade. A autenticação dos geradores de informação (i.e., sensores ou dispositivos IoT) e fundamental para a IoT, pois decisões não podem ser tomadas considerando dispositivos desconhecidos ou não confiáveis” [Cardoso et al. 2022].

Este trabalho e seu artigo base [Cardoso et al. 2022] consideram um ecossistema de uma Cidade Inteligente que envolve diversos atores que se comunicam entre si, consumindo e produzindo dados. O ambiente é composto por gestores da cidade, órgãos públicos, funcionários, sensores e dispositivos IoT. Para melhor entendimento sobre a solução proposta neste artigo, considera-se o cenário de uma CI administrada por órgãos públicos, no qual a administração deseja implantar dispositivos IoT (e.g., sensores, atuadores, câmeras de segurança) para monitorar o ambiente da cidade e fornecer dados para serem consumidos pelo cidadão através de serviços e aplicações. Sem a garantia de que são ıntegros os dados provenientes do sensoriamento de uma cidade inteligente, torna-se inviável para administração tomar decisões estratégicas, atuar sobre o ambiente da cidade ou disponibilizar tais dados para serviços e aplicações.

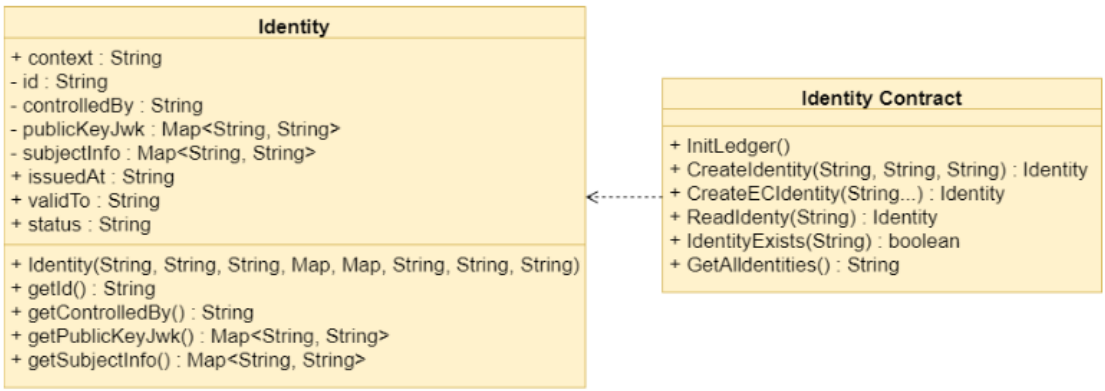

Figura 1. Diagrama de classes referente ao modelo de identidade do artigo base

Neste cenário típico de uma CI, com diversos emissores de informação (i.e., sensores, dispositivos IoT) gerenciados por diferentes entidades administrativas que não se confiam mutuamente, o gerenciamento de identidades deve ser naturalmente descentralizado, e, portanto, pode-se explorar o uso de tecnologias distribuídas como Blockchain. O objetivo deste trabalho e implementar de forma simplificada o modelo do artigo base [Cardoso et al. 2022] para gestão descentralizada de identidades voltado para o domínio de Cidades Inteligentes utilizando a Neo Blockchain [Neo 2022].

2. Modelo proposto

Nesta seção será apresentada, de forma abstraída, a solução proposta e implementada pelo artigo base deste trabalho para o gerenciamento descentralizado de identidades digitais no

contexto das cidades inteligentes.

O modelo de identidades considerará que a Cidade Inteligente deve ser gerida e controlada de forma descentralizada pelas entidades administrativas para manter o ambiente seguro. Serão considerados dois tipos de atores neste ecossistema: entidades administrativas: prefeituras, secretarias e etc; e entidades comuns: funcionários, serviços, sensores, dispositivos IoT etc. As entidades administrativas formam um consórcio que tem o dever de manter a infraestrutura e emissão de identidades da rede Blockchain do ecossistema. Somente entidades que possuem identidade na rede podem ter acesso aos serviços e dados da CI, tornando assim os dados e serviços mais seguros e confiáveis.

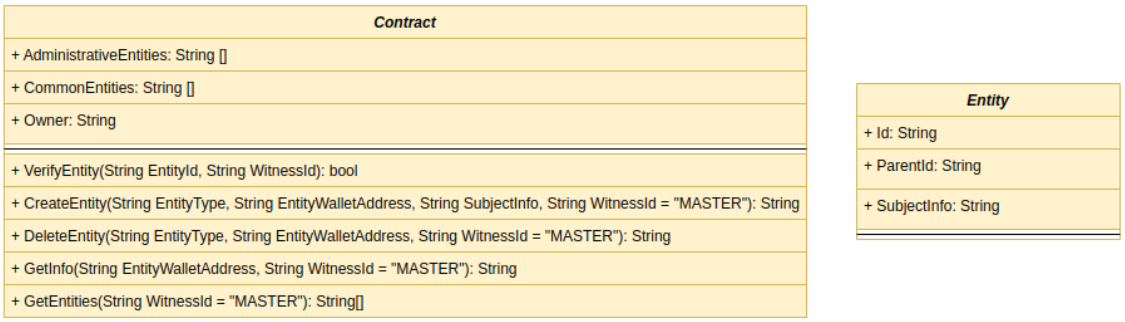

Figura 2. Diagrama das classes Contrato e Entidade na Neo Blockchain

Cada entidade administrativa (EA) tem a função de provedora de identidades, deve gerar sua própria identidade e utilizá-la para gerar a identidade das demais entidades. Ao criar a identidade, a EA deve informar as permissões de escrita/leitura pertinentes a entidade em questão. Assim, há uma hierarquia entre as identidades armazenadas na rede Blockchain, sendo possível verificar a qualquer momento a autenticidade de um dispositivo que tenta, por exemplo, persistir um dado em algum serviço e também rastrear a entidade responsável por sua inclusão no sistema.

3. Desenvolvimento do Contrato Inteligente na Neo Blockchain

Nesta seção discutiremos sobre a implementação do modelo apresentado na Seção 2 na Neo Blockchain. Além disso, veremos como realizar a implantação do contrato na rede da Neo Blockchain.

Para implementação do contrato escolheu-se a rede da Neo Blockchain na versão 3 por ser a mais recente e oferecer suporte a implementação de contratos com uso de oráculos, o que pode ser útil para trabalhos futuros e aperfeiçoamentos da implementação realizada neste trabalho. Além disso, foi escolhida a linguagem C por ter mais suporte na comunidade da Neo Blockchain.

Na Figura 1, vemos o diagrama de classes proposto pelo artigo base. Neste trabalho, para fins de facilitar a implementação de um protótipo usaremos o diagrama de classes simplificado que pode ser visto na Figura 2. A Entidade possuirá apenas seu próprio identificador, o identificador da entidade que a criou e um campo para especificações sobre ela. No contexto da Neo, consideraremos que cada entidade administrativa e cada entidade comum (serviços, sensores, dispositivos IoT) possuem previamente um cadastro/carteira na Blockchain ”pública”, não necessariamente neste consórcio utilizado para

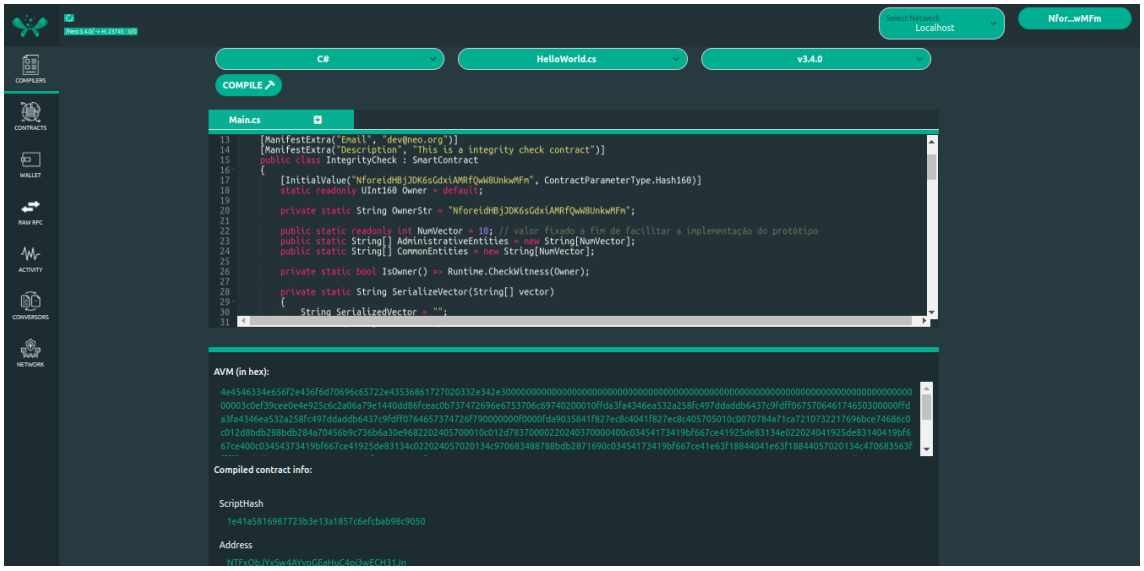

Figura 3. Compilação do código fonte do contrato dentro do ambiente da Neo Blockchain

verificação de identidades. O endereço desta carteira será utilizado como identificador (id e parent id).

Ademais, podemos ver na Figura 2 a classe **Contract**. O Contrato armazenará o identificador de quem o criou, entidade responsável por cadastrar as primeiras entidades administrativas na rede. Além disso, serão armazenados dois vetores: os ids das entidades administrativas e das entidades comuns cadastradas na rede. O contrato proverá cinco funções, Verificação de identidades, criação e remoção de entidades, e obtenção das entidades da rede e suas informações associadas.

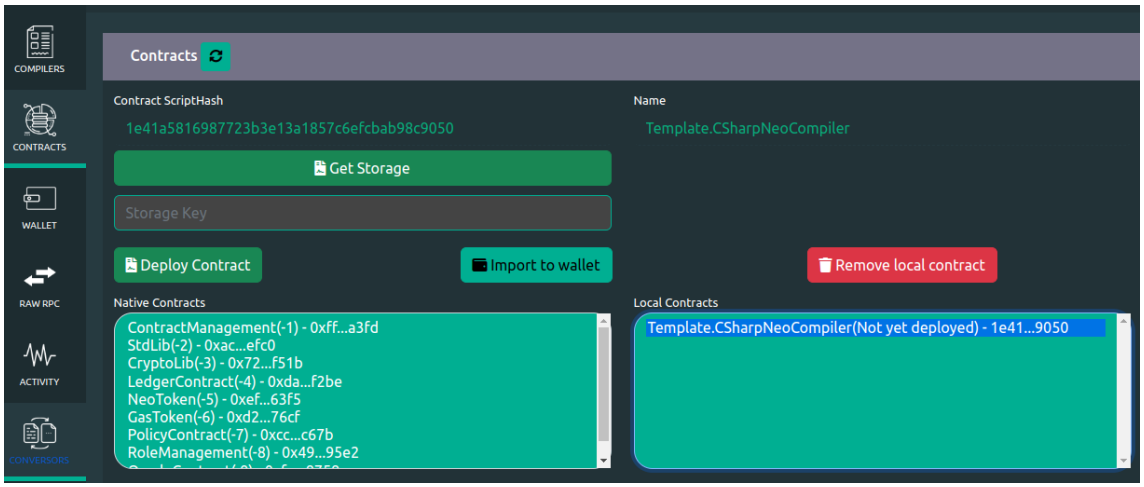

Figura 4. Implantação do contrato na rede

A função verificadora de identidade (**VerifyEntity**) recebe como parâmetro o Id (endereço da carteira) da entidade a qual se deseja verificar a autenticidade e o id da testemunha, ou seja, endereço da carteira de quem estará executando o contrato a fim de verificar uma identidade. Caso a testemunha tenha permissão para realizar essa operação

será retornado um valor booleano que indica se aquela entidade tem um identidade reconhecida pela rede.

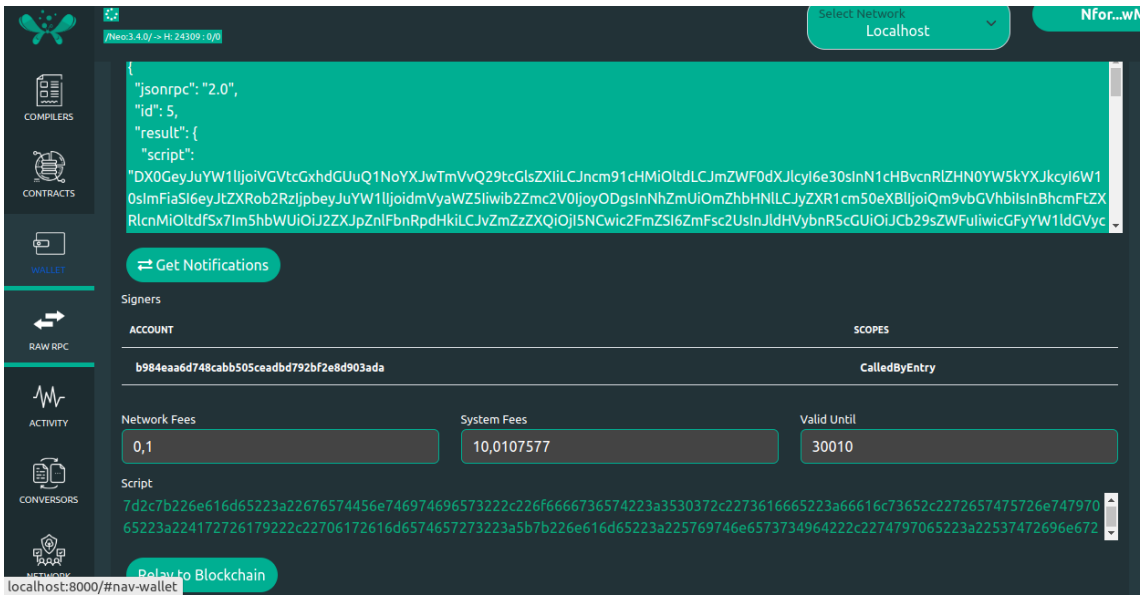

Figura 5. Implantação do contrato na rede

Há também uma função que permite a criação de novas entidades na rede (**CreateEntity**) que recebe como parâmetros o endereço da carteira da entidade a qual se deseja cadastrar, o endereço da carteira do executor do contrato (pai da entidade que será criada), uma descrição com informações sobre a entidade e tipo desta entidade. Caso o executor do contrato seja o Owner do contrato ou seja uma entidade administrativa, ele poderá criar uma nova entidade. É realizada uma verificação do tipo da nova entidade, administrativa ou comum, para que ela possa ser persistida no Storage da rede na lista de permissões apropriada para ela.

Além disso, é possível remover entidades do consórcio (**DeleteEntity**), recuperar o identificador de todas as entidades cadastradas na rede (**GetEntities**) ou recuperar a descrição e entidade pai de uma determinada entidade (**GetInfo**).

O código fonte do contrato inteligente está disponível no GitHub de forma pública [GitHub 2022]. A compilação do código pode ser realizada pelos compiladores da própria Neo Blockchain, como pode ser visto na Figura 3. Após isso, deve ser feita a implantação do contrato na rede. Para tal, acessamos a aba *Contracts* no menu e acionamos o *Deploy Contract* (Figura 4). Depois, há um redirecionamento para a aba *Raw RPC*, onde é possível visualizar quanto será gasto nessa operação. É necessário acionar então o *Relay to Blockchain* (Figura 5) e caso a operação seja bem sucedida o contrato é implantado na rede.

Após a implantação do contrato na rede, ao retornar à aba *Contracts* é possível ver o contrato implantado e cada uma de suas funções públicas, disponíveis para serem executadas por uma testemunha, como ser visto na Figura 5.

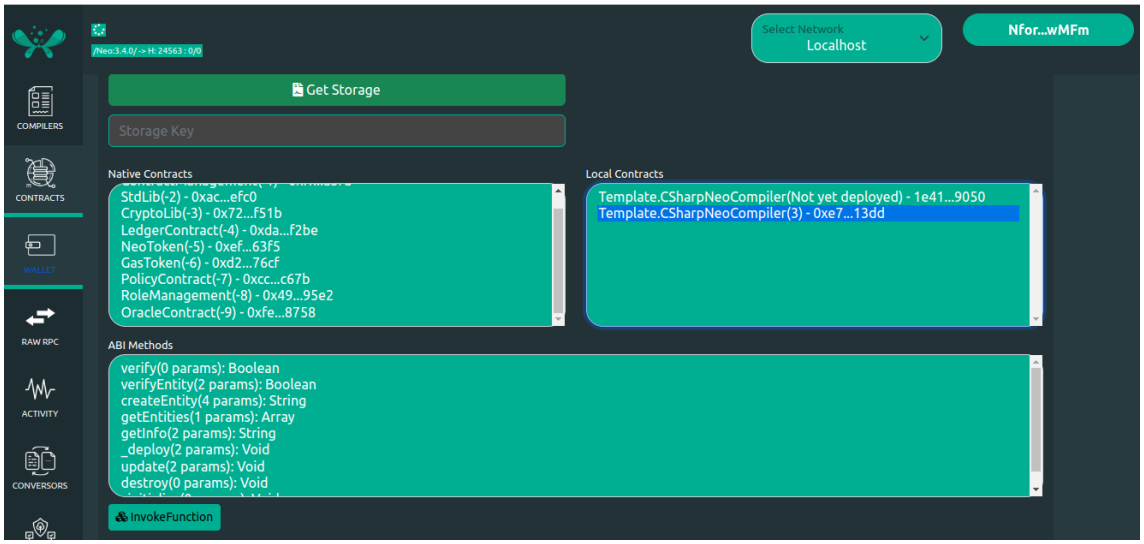

Figura 6. Contrato implantado na rede

4. Conclusão

Cidades Inteligentes vêm se tornando cada mais populares para tornar cidades mais eficientes e sustentáveis. Órgãos públicos podem se beneficiar do uso de sensores e dispositivos IoT para a tomada rápida e eficiente de decisões para a cidade. No entanto, para que isso ocorra, é necessário que os dados gerados por sensores e dispositivos IoT sejam confiáveis, por exemplo. Disso, nota-se a importância de verificar de forma precisa a autenticidade de um dispositivo na rede. Existem entidades administrativas de diversas naturezas numa cidade, é algo naturalmente descentralizado. Por isso, é possível se beneficiar do uso de blockchain para persistir as entidades existentes de forma a tornar o processo de verificação de identidades confiável e auditável.

Neste trabalho foi apresentado um modelo de gerenciamento de identidades digitais utilizando a Neo Blockchain voltado para o contexto de cidades inteligentes. Não foi possível colocar o código em funcionamento para avaliação de seu desempenho pois houveram problemas na execução de algumas funções relacionados ao tratamento de strings e persistência de tipos de dados diferentes de string no código c do contrato. Como trabalho futuro, a ideia é que isso seja solucionado.

Referências

Alamer, M. and Almaiah, M. A. (2021). Cybersecurity in smart city: A systematic mapping study. In *2021 International Conference on Information Technology (ICIT)*, pages 719–724. IEEE.

Cardoso, A. L., Rotondaro, B., Penha, L., Endler, M., da Conceição, A. F., and da Silva e Silva, F. J. (2022). Gerenciamento descentralizado de identidades para cidades inteligentes baseado na tecnologia blockchain. In *Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 57–70, Porto Alegre, RS, Brasil. SBC.

GitHub (2022). Iot integrity check. Disponível em: https://github.com/valescamoura/iot-integrity-check-neoblockchain. Acesso em Dezembro de 2022.

Neo (2022). Neo smart economy. Disponível em: https://neo.org/. Acesso em Dezembro de 2022.

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., and Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(3):2794–2830.