Revista Terra & Cultura: Cadernos de Ensino e Pesquisa

ISSN 0104-8112

APLICAÇÃO DE BLOCKCHAIN EM IDENTIDADES AUTOSSOBERANAS VISANDO CIDADES INTELIGENTES

BLOCKCHAIN APPLICATION ON SELF-SOVEREIGN IDENTITIES TARGETING SMART CITIES

Guilherme Augusto Rocha Manhani[1]
Marc Antônio Vieira de Queiroz[2]

RESUMO

A utilização de infraestrutura e serviços baseados em tecnologia da informação e comunicação é chamada de Cidades Inteligentes. O objetivo do trabalho foi realizar um estudo de caso sobre identidades digitais (ID) e a possibilidade de implementar uma ID única no Brasil utilizando a blockchain para autenticá-la. A metodologia é uma revisão da literatura, nela comparamos as IDs em diferentes países, elencando os resultados positivos da sua implementação. O resultado obtido foi com a utilização da blockchain da rede ethereum com ela se mostrou possível implementar uma ID em um aplicativo de celular inteligente que torna o usuário dono de sua ID, centralizando seus dados e possibilitando compartilhá-los da forma que desejar.

Palavras-chave: Blockchain. Smartcity. Ethereum. Identidade digital.

ABSTRACT

The use of infrastructure and services based on information and communication technology is called Smart Cities. The objective of this work was to conduct a case study on digital identities (ID) and the possibility of implementing a unique ID in Brazil using the blockchain to authenticate it. The methodology is a literature review, in which we compare the IDs in different countries, listing the positive results of its implementation. The result was that using the ethereum network blockchain, it has been shown that it is possible to implement an ID in a smart phone application that makes the user the owner of their ID, centralizing their data and allowing them to share it the way they want.

Keywords: Blockchain. Smartcity. Ethereum. Digital identity.

[1] Graduando em Ciência da Computação, Centro Universitário Filadélfia –Unifil. Departamento de Computação. Londrina –Paraná –Brasil. 86020-000 –guilherme_manhani@edu.unifil.br
[2] Docente do Centro Universitário Filadélfia – Unifil. Departamento de Computação. Londrina – Paraná – Brasil. 86020-000 – marc.queiroz@unifil.br

INTRODUÇÃO

A partir dos anos 2000 o assunto sobre Cidades Inteligentes tem ganhado destaque na computação, muitos estudos foram desenvolvidos e vários avanços tecnológicos foram implementados nas cidades.

Partindo deste conceito o presente trabalho tentará promover a ideia de uma identidade única e digital que melhore a qualidade de vida dos indivíduos, poupando seu tempo e cortando gastos.

Desde meados de 2010, testemunhamos o crescimento constante do inte-resse sobre blockchain, impulsionado pelo sucesso do bitcoin e, mais recentemente,da ethereum. Isso fomentou a pesquisa sobre vários aspectos da tecnologia blockchain, desde seus fundamentos teóricos, criptográficos, econômicos e até sua segurança e privacidade.

Xie *et al*. (2019) relata que segundo a Organização das Nações Unidas (ONU), nos próximos 30 anos, aproximadamente 2,5 bilhões de pessoas se mudem para as cidades, representando 70% da população em centros urbanos.

Com a transformação digital e o surgimento de novas tecnologias podemos resolver problemas, melhorando a qualidade de vida da população, reduzindo gastos desnecessários do Estado, tornando as cidades e os governos mais funcionais e inteligentes.

Desde o surgimento da bitcoin vimos uma ampla gama de aplicações financeiras, bem como uma série de empresas globais adotando a tecnologia blockchain para vários serviços. Essa tecnologia, um tipo de registro distribuído, pode ser especialmente adequada para processar dados ordenados pelo tempo, abrindo assim um leque de aplicações em cidades inteligentes.

Na tentativa de melhorar a governança o presente estudo pretende realizar uma investigação de como a blockchain pode ajudar a resgatar a credibilidade do governo, melhorando a administração nas cidades, promovendo uma economia de recursos públicos, tornando o governo menos burocrático e mais confiável.

DESENVOLVIMENTO

Vivemos na convergência de dois fenômenos relevantes na história da humanidade: a aceleração da urbanização global e a revolução digital. A complexidade da gestão do desenvolvimento urbano sustentável exige soluções nas áreas de educação, saúde, segurança,

transporte, energia, saneamento e outros setores desafiadores, com o crescimento populacional nos próximos anos (TANAKA; BARROS; MENDES, 2018).

Se as iniciativas de infraestrutura forem planejadas corretamente, elas podem resultar em economia de custo na prestação de serviços, graças a economias de escala e podem ter impactos positivos inestimáveis (RAZAGHI; FINGER, 2018).

A tecnologia blockchain poderia reverter o equilíbrio de poder de governos autocráticos para uma situação de "governos como prestadores de serviços", que competem por clientes, propondo propostas de valor para serviços cívicos (SWAN, 2018).

No início, blockchain era usada apenas para transações monetárias e comércio, mas estudos começaram a sugerir que ela poderá ser usada em muitas outras áreas ao longo do tempo, porque há um alto grau de transparência nesse sistema. Por exemplo, no bitcoin, como as carteiras estão em uma estrutura distribuída, a quantidade total de moedas e volume instantâneo de transações no mundo podem ser seguidas momentânea e claramente. Não há necessidade de uma autoridade central para aprovar ou concluir as operações neste sistema baseado em rede peer-to-peer (P2P) (YAVUZ *et al*., 2018).

Blockchain é uma tecnologia de banco de dados distribuída, desenvolvida a partir do bitcoin e outras criptomoedas. Esta tecnologia foi aplicada pela primeira vez no bitcoin, criptomoeda criada por Satoshi Nakamoto em 2008. A blockchain é essencialmente um banco de dados compartilhado, descentralizado e publicamente disponível. Na blockchain, todas as transações são registradas e qualquer pessoa no sistema tem permissão para acessar, enviar e verificar essas transações (XIE *et al*., 2019).

A única maneira de confirmar a ausência de uma transação é estar ciente de todas as transações. A casa da moeda estava ciente de todas as transações e decidiu qual delas chegava primeiro. Para conseguir isso sem uma parte confiável, as transações devem ser anunciadas publicamente, e precisamos de um sistema para os participantes concordem em um único histórico da ordem em que foram recebidos. O beneficiário precisa provar que, no momento de cada transação, a maioria dos nós concordou que foi a primeira recebida (NAKAMOTO, 2008).

Muito se espera da tecnologia blockchain, principalmente em IoT. Um dos principais problemas em IoT é o crescimento contínuo de dispositivos gerando grande tráfego na rede gerando problema de processamento, segurança e armazenamento de informações. Com uma rede P2P a blockchain tem potencial para gerenciar e proteger os dados dessas aplicações.

A arquitetura segura, confiável e descentralizada, é usada para criar esquemas de pagamento seguros e invioláveis, que podem servir as economias e sociedades sem partes

confiáveis. No entanto, a transparência e a rastreabilidade da blockchain restringem severamente o anonimato dos participantes no mundo real, o que causará o vazamento de privacidade dos participantes (ZHANG *et al*., 2018).

As aplicações de blockchain são inúmeras, podemos estar vivenciando o nascimento e amadurecimento de uma tecnologia que em poucos anos estará por trás de praticamente todas as aplicações do nosso cotidiano.

Os serviços de identidades centralizadas que existem hoje falham na forma transparente e de proteção dos direitos dos usuários. Vários desses riscos podem ser evitados usando a tecnologia blockchain. Um estudo literário deixou claro que essa tecnologia pode agregar valor significativo ao gerenciamento de identidades ao devolver a propriedade da identidade ao indivíduo como proprietário dessa identidade. Além disso, a combinação de gerenciamento de identidade com a tecnologia blockchain permite o armazenamento de identidade descentralizado, evitando uma autoridade de autenticação central e impede a violação das identidades e dos dados armazenados (HADDOUTI; KETTANI, 2019).

Imagine um contrato inteligente descentralizado que busque autenticação de endereço, comprovante de situação cadastral (CPF), nome e sobrenome, que transfira dinheiro de uma carteira digital para outra por um aplicativo, apenas usando um clique através de assinatura digital que pode reconhecer sua biometria e face, comprovando a veracidade dos dados do usuário. Isto reduziria fraudes, aumentaria a transparência de transações, seria conivente para o usuário e prestadores de serviços, reduziria custos e evitaria uma série de riscos.

Enquanto a maioria das pessoas se concentra apenas em criptomoedas, na verdade, muitas operações administrativas, procedimentos de Empresas de Tecnologia Financeira (fintech) e serviços cotidianos que só podem ser feitos pessoalmente, agora podem ser movidos com segurança para a Internet como serviços online. O que o torna uma ferramenta poderosa para digitalizar serviços cotidianos é a introdução de contratos inteligentes, como na plataforma ethereum (YAVUZ *et al*., 2018).

O melhor local para se firmar um contrato inteligente é na plataforma da ethereum, que possui código aberto e disponibilização de uma rede descentralizada, assim qualquer pessoa pode desenvolver sua aplicação adequando o mesmo as suas necessidades.

O ethereum é muito mais que uma blockchain e protocolo de criptomoeda. Ele define uma plataforma de programação completa e um ambiente de tempo de execução chamado Ethereum Virtual Machine (EVM). O EVM pode executar os bytecodes de contratos

inteligentes. Um contrato inteligente é um programa que é executado no blockchain e tem sua execução correta imposta pelo protocolo de consenso (HEGEDUS, 2018).

Quando executado, o contrato se torna um programa auto operacional que executa automaticamente condições específicas do contrato se as condições do contrato forem atendidas. Na blockchain os contratos inteligentes permitem que o código seja executado exatamente como programado, sem qualquer possibilidade de fraude ou interferência de terceiros, facilitando a troca de dinheiro, propriedade, ações ou qualquer coisa de valor. Quando você cria um contrato inteligente você pode dizer o que ele faz, por exemplo, transferir tokens, acompanhar saldo, etc. É simples, porém quando criado um contrato inteligente e implantado ele não pode mais ser alterado caso contenha um erro ele não poderá ser consertado, assim se faz necessário validar o código antes de implantá-lo.

O contrato inteligente TheDAO é um exemplo clássico de danos que podem ser causados por um contrato inteligente com vulnerabilidades críticas. Uma exploração de um bug neste contrato levou a uma perda de 60 milhões de dólares em junho de 2016 (HEGEŐUS, 2018).

A execução automática de contratos inteligentes pode eliminar a intervenção humana no comércio, o que minimiza os riscos potenciais de segurança e privacidade (LUO *et al.*, 2019).

Segundo Torres *et al*. (2016) o cartão eID começou a ser usado na Estônia no ano 2002, atualmente ele é controlado pela polícia por um sistema público privado e são válidos por 5 anos, tem suporte a transações eletrônicas e podem ser usado para identificação civil, documento de viagem e serviços médico, bancário e de votação. Na Estônia a outra solução é um ID móvel que permite autenticação nos serviços de E-Gov e assinatura de contratos eletrônicos, tudo acessado por uma senha pessoal.

O governo federal brasileiro não reconhece o cidadão como todo, devido a existência de vasta documentação e ao fato de cada órgão do governo ter o seu datacenter, o seu banco de dados e suas regras. Isto leva os órgãos a reconhecerem o indivíduo de forma fragmentada.

O Brasil é um país continental muito populoso e muito extenso em território, o que torna difícil a implementação de uma identidade única e centralizada, além do grande nível de corrupção e fraude. É inviável segundo Torres *et al.* (2016) a confecção de cartão eID como na maiorias dos países estudados por ele, devido a lei federal o governo é responsável por arcar com o custo de emissão da primeira via de um documento, com o custo de 40 reais por cartão a emissão para cada cidadão teria uma despesa de mais de 8 bilhões de reais para o governo,

Torres *et al.* (2016) ainda aponta a existência de uma baixa adesão dos usuários ao cartão eID nos países que foram implementados.

O eID móvel é uma solução viável de implementar no Brasil, segundo Meirelles (2019) temos mais de 1 celular inteligente por habitante no Brasil, são 230 milhões em uso no país, se somarmos os notebooks e tablets são 324 milhões de dispositivos isto em maio de 2019, o que dá 1,6 aparelhos por habitante. Este dado mostra que a solução deve partir de aplicativo móvel depois para web, visto que hoje no Brasil o acesso a celulares inteligentes abrangem grande parte da população.

Implementar a ID soberana mantém a independência dos órgãos público, armazenando informações dos usuários na blockchain. Está tecnologia tem a capacidade de transformar os bancos de dados do governo em o banco de dados dos usuários. Estas informações seriam autenticadas pelo estado ou terceiro confiável, tornando os usuários donos de sua ID. A solução pode ser implementada por iniciativa pública ou parceria pública privada, visto que será necessário fazer reivindicação em um banco de dados do governo.

É importante levar em conta plataformas já existentes como uPorte e Self-Sovereign que dão base na implementação de ID trazendo ferramentas e protocolos que criam aplicativos centrados no usuário e descentralizados, não sendo necessário partir do zero na implementação, pois são padrões aberto de código.

A ID soberana tem credenciais as quais atestam a veracidade dos documentos nela existente, por exemplo, credencial de direção, credencial de nacionalidade entre outras. Existe permissionamento nesta ID, isto significa que ela pertence ao usuário o qual vai escolher como compartilhar seus dados ou seja, você pode comprar algo e para isso precisa provar que tem o dinheiro, mas não o quanto tem, assim mantemos a confiança e ocultamos as informações sensíveis.

Nos últimos anos o Brasil vem evoluindo o seu governo digital, Rodrigues (2019) mostra em reportagem que no dia 6 de setembro o presidente Jair Bolsonaro assinou uma medida provisória (MP) que cria a carteirinha estudantil digital que será distribuída de forma gratuita em aplicativos de celulares ou pela Caixa Econômica Federal em forma física.

Lis (2019) mostra outra iniciativa: A carteira de trabalho digital, que tira a necessidade da escrita na carteira física, as informações serão migradas da plataforma eSocial. Entretanto não faz sentido migramos de vários documentos físicos para virtuais, a solução não resolve o problema do cidadão ser conhecido de forma fragmentada

Em 2017 o ministério do planejamento fez uma prova de conceito em parceria com a Microsoft, uPort e Consensys de uma ID que foi bem sucedida, segundo Ministério do Planejamento (2018) um projeto piloto está sendo conduzido pelo Tribunal Superior Eleitoral (TSE) e deveria estar disponível para toda a população em julho de 2018, está solução traria a integração do título de eleitor e CPF. E futuramente inclusão da Carteira Nacional de Habilitação (CNH), cartão saúde, certidão de nascimento e casamento.

Pelos argumentos apresentados e as tecnologia levantadas neste estudo a solução viável para criação de um ID soberana é através do desenvolvimento de um aplicativo de celular usando contrato inteligente aplicado a blockchain da ethereum com validação de credenciais por bancos de dados de órgãos governamentais ou terceiro confiáveis, o cidadão será dono de sua ID limitando as informações que ele julgar sensíveis.

CONCLUSÃO

Com o surgimento das criptomoedas e seu sucesso testemunhamos o nascimento da tecnologia blockchain que pode mudar radicalmente nosso mundo devido a inúmeras aplicações possíveis desta tecnologia. Utilizando esta inovação tecnológica podemos tornar o governo mais inteligente, transparente e menos burocrático.

O E-Gov brasileiro tem melhorado, porém o cidadão ainda não é reconhecido como um todo. Outros países ao redor mundo, implementaram soluções diferentes para seus governos, porém segundo teóricos do tema, no Brasil, ainda seria inviável a confecção de um cartão eID por cidadão devido ao alto custo e a baixa adesão. Podemos observar, no entanto, que como países da África, o Brasil saltou a tecnologia dos computadores para celulares inteligentes. E através da rede ethereum usando padrões de código aberto é possível implementar uma ID autossoberana descentralizada e centralizada no usuário, que seria dono de sua própria ID podendo escolher quais informações ele quer compartilhar. Tudo controlado por um aplicativo de celular, que seriam possíveis de serem replicadas em território nacional.

Ainda há perguntas a serem respondidas sobre as ID, se haverá adesão da população, viabilidade financeiramente e se realmente vão facilitar a vida do usuário ou se tornarão um problema físico em um problema virtual, mais estudos precisam continuar a serem fomentados para que questões como as citadas possam ser sanadas e possíveis problemas possam ser corrigidos.

REFERÊNCIAS

HADDOUTI, S. E.; KETTANI, M. D. E. C. E. Analysis of identity management systems using blockchain technology. In: INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION TECHNOLOGIES AND NETWORKING (CommNet), 2019, Rabat, Morocco. **Proceedings** […]. Rabat, Morocco, IEEE, 2019. Disponível em: https://doi.org/10.1109/commnet.2019.8742375. Acesso em: 29 jun. 2020.

HEGEDUS, P. Towards analyzing the complexity landscape of solidity based ethereum smart contracts. In: INTERNATIONAL WORKSHOP ON EMERGING TRENDS IN SOFTWARE ENGINEERING FOR BLOCKCHAIN – WETSEB, 1., 2018, Gothenburg, Sweden. **Proceedings** […]. Gothenburg, Sweden: ACM Press, 2018.

LEE, J. H. BIDaaS: Blockchain based ID as a service. **IEEE Access, Institute of Electrical and Electronics Engineers** (IEEE), South Korea, v. 6, p. 2274–2278, 2018.

LIS, L. **Governo publica regras para emissão da carteira de trabalho digital**. 2019. Disponível em: https://g1.globo.com/economia/noticia/2019/09/24/governo-publica-regras-para-emissao-da-carteira-de-trabalho-digital.ghtml. Acesso em: 29 jun. 2020.

LUO, X. et al. A payment channel based hybrid decentralized ethereum tokenex change. In: IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019. **Proceedings** […]. Seoul, Korea: IEEE, 2019.

MEIRELLES, F. S. **30ª pesquisa anual do uso de TI nas empresas, 2019**. FVG, 2019. Disponível em: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/pesti2019fgvciappt_2019.pdf. Acesso em: 29 jun. 2020.

BRASIL. Ministério do Planejamento. **Documento Nacional de Identidade.** 2018. Disponível em: http://www.planejamento.gov.br/assuntos/tecnologia-da-informacao/documento-nacional-de-identidade/dni-1. Acesso em: 29 jun. 2020.

NAKAMOTO, S. **Bitcoin**: A peer-to-peer electronic cash system. 2008. Disponível em: http://bitcoin.org/bitcoin.pdf. Acesso em: 29 jun. 2020.

RAZAGHI, M.; FINGER, M. Smart governance for smart cities. **Proceedings of the IEEE, Institute of Electrical and Electronics Engineers (IEEE),**. [*S.l.*], v. 106, n. 4, p. 680–689, apr. 2018.

RODRIGUES, M. **Bolsonaro assina mp que cria carteirinha estudantil digital, emitida pelo governo.** 2019. Disponível em: https://g1.globo.com/educacao/noticia/2019/09/06/bolsonaro-assina-mp-que-cria-carteirinha-estudantil-digital-emitida-pelo-governo.ghtml. Acesso em: 29 jun. 2020.

SWAN, M. Blockchain enlightenment and smart city cryptopolis. In: WORKSHOP ON CRYPTOCURRENCIES AND BLOCKCHAINS FOR DISTRIBUTED SYSTEMS – CryBlock, 1., 2018. **Proceedings** […]. [*S.l.*]: ACM Press, 2018.

TANAKA, S. A.; BARROS, R. M.; MENDES, L. S. A proposal to a framework for governance of ICT aiming at smart cities with a focus on enterprise architecture. **Brazilian Symposium on Information Systems** – SBSI, [*S.l.*], v. 52, n.1, p. 52-58, 2018.

TORRES, J. A. S. et al. National strategy of identity management to boost brazilian electronic government program. In: LATIN AMERICAN COMPUTING CONFERENCE (CLEI), 42., 2016, Valparaiso. **Proceedings** […]. Valparaiso: IEEE, 2016.

XIE, J. et al. A survey of blockchain technology applied to smart cities: Research issues and challenges. **IEEE Communications Surveys & Tutorials**, [*S.l.*], v. 21, n. 3, p. 2794-2830, 2019.

YAVUZ, E. et al. Towards secure e-voting using ethereum blockchain. In: INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSIC AND SECURITY (ISDFS), 6., 2018, Antalya. **Proceedings** […]. Antalya: IEEE, 2018.

ZHANG, D. et al. An anonymous off-blockchain micropayments scheme for cryptocurrencies in the real world. **IEEE Transactions on Systems, Man, and Cybernetics**: Systems, [*S.l.*], v. 50, n. 1, p. 32-42, jan. 2020.