

**DANIEL SOARES DO NASCIMENTO NETO
FELIPE GUZEN SPERB**

**ESTUDO SOBRE A BLOCKCHAIN E SUA APLICAÇÃO EM IDENTIDADES
DIGITAIS**

**Ji-Paraná
2023**

**DANIEL SOARES DO NASCIMENTO NETO
FELIPE GUZEN SPERB**

**ESTUDO SOBRE A BLOCKCHAIN E SUA APLICAÇÃO EM IDENTIDADES
DIGITAIS**

Trabalho de Conclusão de Curso
apresentado ao Centro Universitário
São Lucas Ji-Paraná como requisito
parcial para obtenção do Título de
Bacharel em Sistemas de Informação.
Prof. Orientador: Esp. Romário Vitorino
Ferreira

**Ji-Paraná
2023**

Dados Internacionais de Catalogação na Publicação - CIP

N244e	Nascimento Neto, Daniel Soares do. Estudo sobre a blockchain e sua aplicação em identidades digitais. / Daniel Soares do Nascimento Neto; Felipe Guzen Sperb. – Ji-Paraná, 2023. 18 p.; il. Trabalho de Conclusão de Curso (Sistemas de Informação) – Centro Universitário São Lucas Ji-Paraná, 2023. Orientador: Prof. Esp. Romário Vitorino Ferreira. 1. Blockchain. 2. Identidades digitais. 3. Segurança digital. I. Sperb, Felipe Guzen. II. Ferreira, Romário Vitorino. III. Título. CDU 336.7:004
-------	--

AGRADECIMENTOS

Eu, Daniel Soares, agradeço minha família, amigos e minha namorada por toda confiança e apoio prestado durante esse tempo.

Eu, Felipe Guzen, agradeço a minha família, amigos e todos que contribuíram para minha formação ao longo desses anos.

Agradecemos principalmente a Deus, por toda força e sabedoria que nos forneceu durante os semestres, nos conduzindo em cada situação da melhor forma possível.

Ao professor Romário Vitorino, nossa mais sincera gratidão pelas dicas e auxílio durante esta fase, e por sua amizade.

Aos professores, coordenadores e colegas, muito obrigado por cada troca de informação fora e dentro da sala de aula.

Somos gratos aqueles que de alguma forma estiveram e estão próximos de nós, fazendo esta vida valer cada vez mais a pena.

SUMÁRIO

1	INTRODUÇÃO.....	08
2	MATERIAL E MÉTODOS.....	09
3	RESULTADOS E DISCUSSÃO.....	10
3.1	Introdução à Tecnologia Blockchain.....	10
3.2	Desafios da Identidade Digital Tradicional.....	12
3.3	Blockchain como Solução para Identidade Digital.....	13
3.4	Ethereum.....	13
3.5	Casos de Uso.....	14
4	CONCLUSÃO.....	17
5	REFERÊNCIAS BIBLIOGRÁFICAS.....	18

RESUMO

A blockchain, um conceito que teve seu início no ano de 2008 por Satoshi Nakamoto, onde o autor destaca um processo que permitiria a criação de uma moeda digital e sua transação de forma confiante e segura sem a necessidade de intermediários, se tornando uma tecnologia disruptiva explorada na atualidade em diversas áreas que vai além do ramo financeiro. Dessa forma, o aprofundado neste artigo traz informações sobre a tecnologia blockchain e como ela contribui para garantir a segurança dos dados, descentralização das informações e confiabilidade, mostrando também os desafios atuais no gerenciamento de identidades digitais, e a solução através da blockchain. O método utilizado foi uma revisão integrativa da literatura que visou o levantamento de conceitos e aplicações dessa tecnologia à identidades digitais, utilizando descritores de busca que incluíram as palavras-chave relevantes, como "blockchain", "identidades digitais", "gestão de identidades" e "segurança digital". Através dessa metodologia, foi possível discutir como surgiu a blockchain, seus principais fundamentos e aplicação, se voltando para a resolver a problemática encontrada nos tradicionais gerenciamentos de identidade, trazendo conhecimento sobre identidades auto-soberanas descentralizadas. Dessa forma, foi possível apresentar a tecnologia e como essa pode resolver os impasses que envolvem a identificação digital resolvendo os principais problemas de confiabilidade e integridade.

Palavras chave: Blockchain. Identidades digitais. Segurança digital.

ABSTRACT

Blockchain, a concept that began in 2008 by Satoshi Naskamoto, where the author highlights a process that would allow the creation of a digital currency and its transaction in a confident and secure way without the need for intermediaries, is a disruptive technology explored today in several areas that go beyond the financial sector. In this way, this article provides information on blockchain technology and how it contributes to ensuring data security, decentralization of information and reliability, also showing the current challenges in managing digital identities, and the solution through blockchain. The method used was an integrative literature review that aimed to survey the concepts and applications of blockchain to digital identities, using search descriptors that included the relevant keywords, such as "blockchain", "digital identities", "identity management" and "digital security". Through this methodology, it was possible to discuss how blockchain emerged, its main foundations and application, turning to solve the problem found in traditional digital identity management, bringing knowledge about decentralized self-sovereign identities. In this way, it was possible to present the technology and how it can solve the impasses surrounding digital identification by resolving the main problems of reliability and integrity.

Keywords: Blockchain. Digital identities. Digital security.

1. INTRODUÇÃO

A partir do século XX surgiu um conceito denominado “Cidade Inteligente”, que é utilizado para definir as cidades que possuem infraestrutura e serviços baseados em tecnologia da informação e comunicação entre dispositivos. Com o crescimento da internet das coisas (IoT), que promove a interconexão digital de objetos cotidianos com a internet, permitindo que eles coletam e transmitem dados, as cidades inteligentes se tornando cada vez mais presente em nosso cotidiano, porém, como apontado por Chicarino et al. (2017) esse crescimento além dos benefícios, trazem também maiores exposições a ameaças de segurança e privacidade.

No entanto, existe uma tecnologia disruptiva que pode oferecer soluções para esse desafio: a blockchain. Teorizada inicialmente por Satoshi Nakamoto em 2008, a blockchain é uma tecnologia que surgiu como a base das criptomoedas, a princípio o Bitcoin, mas que tem aplicações em diversas áreas e indústrias. Ela nos afirma a possibilidade de se ter cada vez mais serviços digitais seguros, e isso vem graças a diversos outros processos tecnológicos que erguem os pilares da blockchain, sendo a imutabilidade, a descentralização, e a transparência, proporcionando confiança de forma que, “Não há necessidade de uma autoridade central aprovar ou concluir as operações neste sistema baseado em P2P” (YAVUZ et al., 2018).

Tal tecnologia vai muito além do grande potencial de garantir segurança de informações, mas também é a base para o conceito de *smart contracts*, que oferece possibilidades de desenvolver regras de negócios para contribuir com uma nova forma de visualizar o mundo.

Entendendo essa grandeza, este trabalho teve foco em identidade digital, enfatizando a combinação de gerenciamento de identidade com a blockchain, pois assim se tem o armazenamento descentralizado da identidade evitando uma autoridade de autenticação central, inviabilizando as possibilidades de adulterações das identidades e dados (EL HADDOUTI; EL KETTANI, 2019).

Contudo, serão apresentados os conceitos e características fundamentais do blockchain, como ela contribui para garantir a segurança dos dados, a descentralização das informações e a confiabilidade. Além de mostrar os desafios presentes no gerenciamento de identidades digitais atuais e os conceitos que envolvem contratos inteligentes.

2. MATERIAL E MÉTODOS

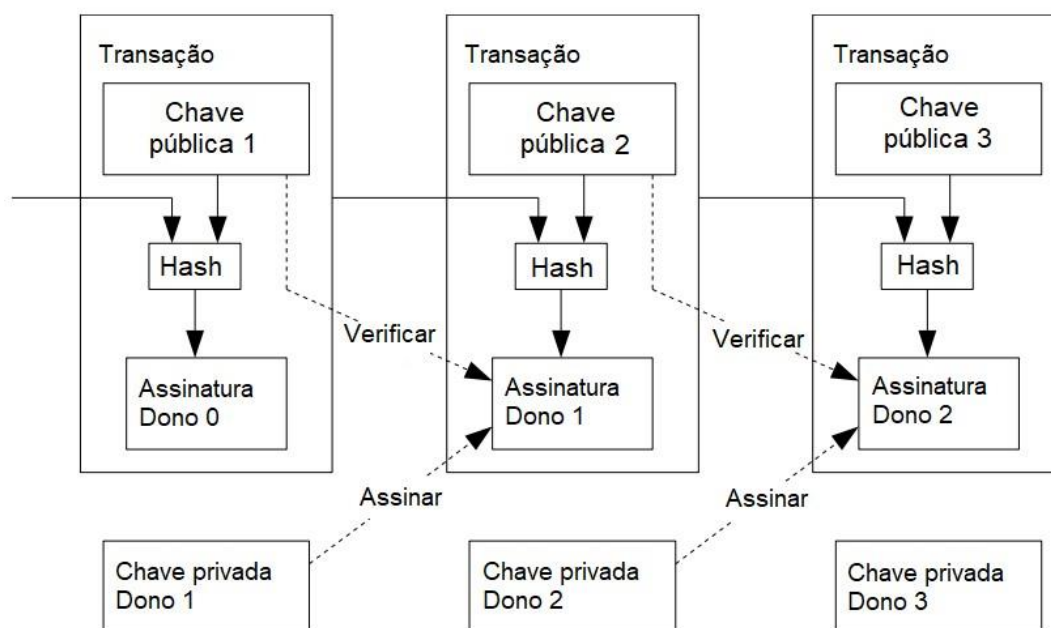
Para o desenvolvimento desta pesquisa, efetuou-se uma revisão integrativa da literatura. As fases desta revisão integrativa foram: definição do tema e desenho do estudo, critérios para a seleção dos estudos, pesquisa e avaliação de informações, interpretação dos resultados e produção da revisão. Para a busca de estudos, utilizou-se bases de dados confiáveis, como Google Acadêmico, SciELO, ScienceDirect e SpringerLink. Os descritores de busca incluíram as palavras-chave relevantes, como "blockchain", "identidades digitais", "gestão de identidades" e "segurança digital". Os critérios de inclusão compreendem artigos científicos, incluindo pesquisas originais e revisões, disponíveis eletronicamente, publicados nas línguas portuguesa, inglesa ou espanhola, em periódicos nacionais e internacionais, no período de 2008 a 2022. Os critérios de exclusão abrangem artigos duplicados, dissertações, teses, resumos de conferências e estudos que não estejam diretamente relacionados à problemática desta pesquisa. A busca se conduziu de forma sistemática e devidamente documentada, incluindo a data de realização da pesquisa. Após a seleção dos estudos, seguiu com a extração de informações essenciais, incluindo sobre metodologia, resultados e conclusões. A qualidade metodológica dos estudos foi avaliada para garantir a robustez da revisão. Durante a análise, identificou tendências na literatura, bem como possíveis pontos de convergência e divergência. Por fim, foi realizada uma revisão integrativa, seguindo uma estrutura adequada que inclui introdução, metodologia, resultados, discussão e conclusões. A revisão não só apresenta uma síntese dos principais achados, mas também destaca lacunas na literatura e fornecerá recomendações para pesquisas futuras.

3. RESULTADOS E DISCUSSÃO

3.1. Introdução à Tecnologia Blockchain

A blockchain é uma inovação revolucionária no campo da tecnologia de registro distribuído, pois permite a criação de um livro de registros transparente, seguro e imutável, no qual as transações são gravadas de forma descentralizada, sem a necessidade de uma autoridade central. Sua idealização teve início através de um *white paper* intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System" desenvolvido por Satoshi Nakamoto no ano de 2008. Neste, Nakamoto (2008), descreveu os conceitos-chave por trás da blockchain, definindo o sistema de transação Bitcoin como uma “versão puramente peer-to-peer do dinheiro eletrônico”, de forma a permitir que os pagamentos online sejam enviados diretamente de uma parte para outra sem a necessidade de uma instituição financeira ou de um terceiro de confiança.

Figura 1 - Sistema de transação blockchain



Fonte: adaptado de Nakamoto (2008).

Lucena e Henrique (2016) define a blockchain como uma base distribuída de dados que se mantém em uma cadeia de blocos, obtendo informações de todos os registros dos elementos de uma rede, impossibilitando revisão e adulteração dos mesmos. Esse encadeamento é feito através da função *hash* gerada em cada bloco,

e sempre que um novo for validado, neste, é adicionado a hash do bloco anterior, fazendo com que qualquer alteração ao mínimo que seja, altere todos os blocos. Lima (2022), explica com suas palavras:

“O alinhamento dos blocos de forma cronológica faz com que uma transação não possa ser alterada com antecedência sem alterar seu bloco e todos os blocos a seguir. Esse arranjo de informações permite a segurança e descentralização de dados sem a necessidade de um banco de dados central e pode ser expandido para várias áreas em que a troca de dados e informações é vital”

A respeito das funções *hash*, Lucena e Henrique (2016), conceitua que são funções no qual mapeiam uma entrada de tamanho arbitrário em um conjunto de *bits* de tamanho fixo e totalmente dependentes da entrada, de forma a ser improvável obter a entrada a partir de seu *hash*, além de se ter valores totalmente diferentes para qualquer alteração na entrada, mesmo que de apenas um *bit*.

Esta tecnologia se baseia em princípios essenciais que a diferenciam de sistemas tradicionais. Primeiramente, é totalmente descentralizada, permitindo que qualquer pessoa análise independentemente e valide as transações, conforme um conjunto predeterminado de regras, as quais não podem ser alteradas por ninguém, e são determinadas por uma função matemática, eliminando a vulnerabilidade de um único ponto de falha (FORNASIER, 2022). Cada nó na rede possui uma cópia completa do registro, garantindo a segurança e resistência da rede, assim como definido por Nakamoto (2008).

Outro princípio fundamental é a imutabilidade, significando que uma vez que os dados são registrados em um bloco e adicionados à cadeia, eles se tornam permanentes e não podem ser modificados ou apagados (ALVES et al., 2018). Isso é possível graças a algoritmos de criptografia avançada e ao consenso distribuído aos participantes, que garantem a integridade das transações.

Outro ponto de segurança acrescentado às transações, é a identificação do proprietário da realização de modificações, sendo validado através da assinatura digital, que “por sua vez, visa garantir que toda e qualquer alteração em algum elemento pertencente a determinado nó da rede blockchain foi realizada pelo proprietário do par de chaves pública e privada daquele nó” (LUCENA; HENRIQUE, 2016). Cada usuário possui um par de chaves criptográficas - uma pública e uma privada. A chave pública é usada para criar endereços na rede, enquanto a chave privada é usada para assinar transações, garantindo autenticidade e segurança (CHICARINO et al., 2017).

Com seu potencial disruptivo, a blockchain tem o poder de transformar diversos setores, como o financeiro, logístico e governamental, proporcionando maior eficiência, transparência e segurança nas operações, aumentando os serviços digitais de forma a melhorar a qualidade de vida da população com a redução de gastos desnecessários em terceiros, poupando tempo, tornando as cidades e os governos mais funcionais, inteligentes e seguros (MANHANI; QUEIROZ, 2020).

3.2. Desafios da Identidade Digital Tradicional

A identidade digital tradicional enfrenta uma série de desafios significativos que comprometem a segurança e a privacidade dos usuários em ambientes digitais. Entre os principais desafios, a dependência excessiva de senhas e autenticação de dois fatores (2FA) tem se destacado. Conforme observado por Simmonds (2015) em seu tópico “Porque a identidade digital falha”, as senhas são a forma mais comum de autenticação, porém, com muitas falhas, tendo em vista que precisam ser armazenadas, o que as tornam vulneráveis a ataques. O autor ainda diz que esse método influencia a más práticas no sentido de ser difícil lembrar de muitas senhas diferentes, o que leva a pessoas a usar senhas fáceis de lembrar, que são mais fáceis de quebrar, ou usando a mesma senha para várias contas, o que significa que, se uma senha for descoberta, todas as contas protegidas por ela também serão comprometidas.

Outro desafio relevante é a segurança dos sistemas centralizados de gerenciamento de identidade. Nesse contexto, Manhani e Queiroz (2020) mencionam que os serviços de identidades centralizadas que existem hoje falham na forma transparente e de proteção dos direitos dos usuários, pelo fato de que os armazenamentos centralizados são vulneráveis a ataques cibernéticos, falhas de segurança e violações de privacidade, uma vez que todos os dados são armazenados em um único local. Isso significa que, se um hacker conseguir acessar o sistema, ele pode roubar ou manipular informações pessoais dos usuários, como nome, endereço, número de identificação, entre outros. Além disso, os armazenamentos centralizados são controlados por uma única entidade, o que significa que os usuários não têm controle sobre seus próprios dados e não podem decidir quem pode acessá-los ou como eles são usados. Por essas razões, a tecnologia blockchain e a criação de identidades auto-soberanas descentralizadas são vistas como soluções para esses

problemas, pois permitem que os usuários tenham controle total sobre seus dados e possam compartilhá-los de forma segura e transparente.

3.3. Blockchain como Solução para Identidade Digital

A tecnologia blockchain está se destacando como uma possível solução para os problemas da identidade digital comuns hoje em dia. O que torna a blockchain especial é sua habilidade de criar registros que são compartilhados por todos e não podem ser alterados, sendo fundamental para a criação de sistemas de identidade digital auto-soberanos (SSI) baseados em blockchain. Manhani e Queiroz (2020) enfatiza a que a tecnologia blockchain pode garantir a segurança das identidades digitais ao devolver a propriedade da identidade ao indivíduo como proprietário dessa identidade, permitindo também o armazenamento descentralizado, evitando uma autoridade de autenticação central e impedindo a violação das identidades e dos dados armazenados, resolvendo as problemáticas citadas anteriormente.

A identidade auto-soberana, também conhecida como *self-sovereign identity* em inglês, é um conceito que se refere à utilização de blockchain associado à criptografia para criar uma identidade digital única e exclusiva para cada usuário. Essa identidade é auto-soberana porque o usuário tem total controle sobre ela, podendo decidir quais informações e com quem compartilhar. A arquitetura distribuída e descentralizada utilizada pela maioria dos sistemas de identificação baseados em blockchain oferece mais segurança contra ciberataques, violações de dados e corrupção de dados (BATISTA et al. 2018).

Manhani e Queiroz (2020) também mencionam outros fatores que fortalecem essa segurança, sendo esses a transparência e a rastreabilidade que restringem severamente o anonimato dos participantes no mundo real, o que aumenta a segurança e a privacidade dos dados pessoais dos usuários.

3.4. Ethereum

Ethereum é um importante conceito dentro de aplicações que envolve a blockchain, isso porque não se trata apenas de uma aplicação, mas sim de um conjunto de tecnologias. Yavuz et al. (2018) em suas palavras, diz “O que o torna uma ferramenta poderosa para digitalização serviços diários é a introdução de

contratos inteligentes, como em a plataforma Ethereum”. Esse ambiente permite a criação de aplicativos descentralizados (*dApps*) e contratos inteligentes, que são programas que executam automaticamente as condições estabelecidas em seu código. No conceito de Yavuz et al. (2018), para definir um contrato inteligente é escrito códigos que define regras, objetos, modelos de dados e a partir daí o contrato pode ser executado, sendo que depois que inicializado “não podem ser descartados do blockchain, e as pessoas podem olhar para trás para ver se os resultados da execução de contratos inteligentes são verdadeiros ou não”.

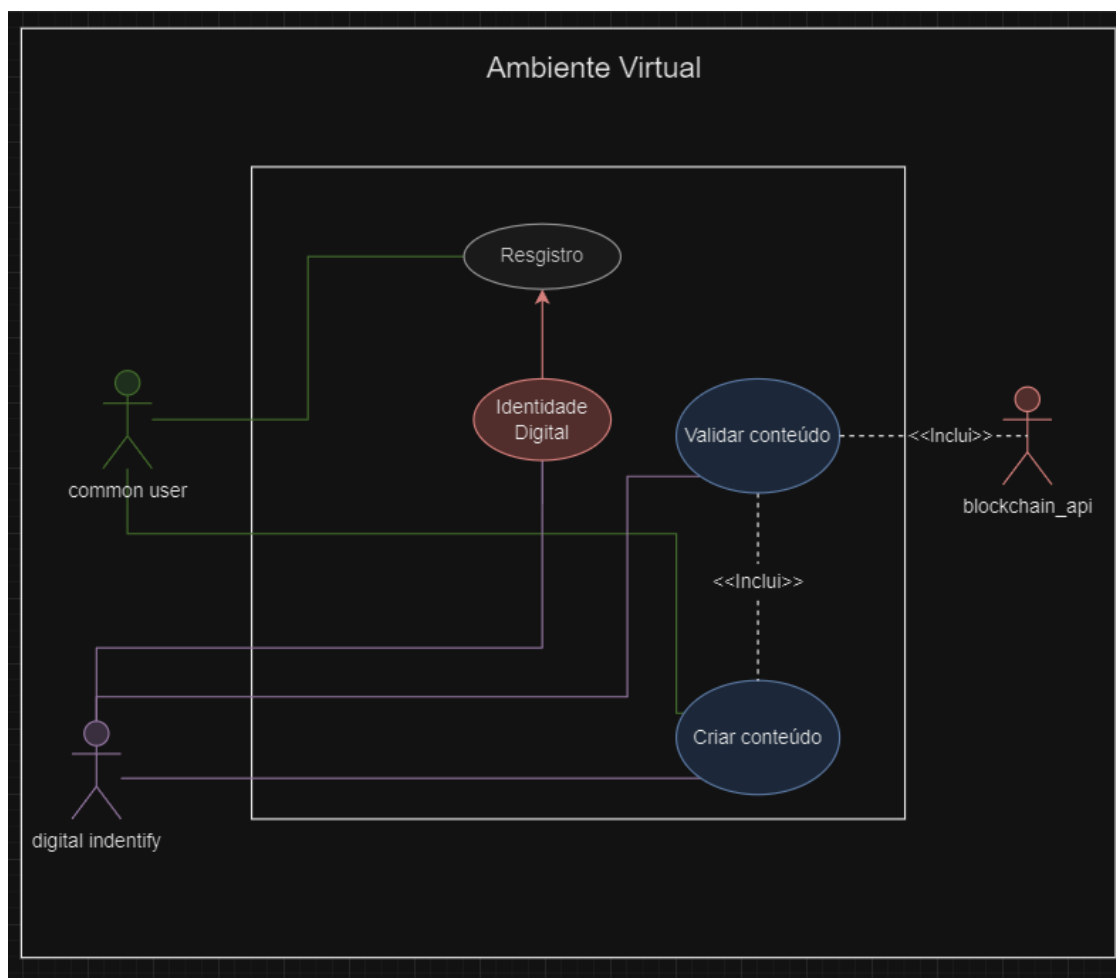
A plataforma Ethereum é baseada em código aberto e disponibiliza uma rede descentralizada, permitindo que qualquer pessoa possa desenvolver sua aplicação adequando o mesmo às suas necessidades. Em resumo, o Ethereum é uma plataforma que permite a criação de aplicativos descentralizados e contratos inteligentes, utilizando a tecnologia blockchain (MANHANI; QUEIROZ, 2020).

3.5. Casos de Uso

Existem vários casos de uso e exemplos práticos que demonstram a eficácia do blockchain na gestão de identidade digital. Como o programa "e-Residency" na Estônia. Costa (2019) explica que a Residência Eletrônica é uma identidade digital que qualquer pessoa no mundo pode obter para participar de uma plataforma baseada em inclusão, legitimidade e transparência. Os residentes eletrônicos, ao receberem sua identificação digital, têm acesso ao mercado europeu e também podem usar serviços públicos eletrônicos. O objetivo principal é que os residentes eletrônicos possam liderar uma empresa confiável na Europa, independentemente de sua localização, com os meios necessários para realizar negócios globalmente.

Já Batista et al. (2018) exemplifica um caso de uso onde se tem dois tipos de usuários: o "*common user*" (usuário comum) e o "*digital identity*" (usuário com identificação digital).

Figura 2 - Caso de uso identificação digital



fonte: adaptado de Batista et al. (2018)

De acordo com a figura 2, o autor explica que o *digital identity* criaria sua identidade digital única e exclusiva em uma plataforma baseada em blockchain que gere essa identificação. Ambos podem realizar cadastros e gerar conteúdos no ciberespaço, porém, o usuário com ID digital terá posse de uma chave privada e outra pública onde com a sua chave pública, poderá ou não marcar seus conteúdos digitais. “A assinatura digital só será validada após ser inserida ao bloco de correntes sequenciadas, imutáveis e transacionais (blockchain_api). Sua chave privada estabelecerá a autenticidade do conteúdo gerado.” (BATISTA et al. 2018).

Na prática, a partir daí, ele pode utilizar essa identificação para realizar transações financeiras, acessar serviços online, compartilhar informações com outras pessoas ou empresas, entre outras possibilidades, onde a plataforma blockchain garante a segurança e a confiabilidade dessas transações, uma vez que os registros são imutáveis e descentralizados, o que dificulta a ocorrência de fraudes ou violações

de dados, além de inibir a necessidade de passar dados pessoais como nome, email, CPF. (BATISTA et al. 2018).

Yavuz et al. (2018) em seu artigo menciona o projeto Sovrin, onde o define como: “é um consórcio Blockchain onde todos podem utilizar a plataforma, sem autorização prévia”. O autor nos explica que a rede é governada por uma fundação sem fins lucrativos, e os nós validadores são selecionados por um processo transparente. Cada usuário do Sovrin tem uma identidade única, chamada de identificador descentralizado (DID). Os DIDs são criados por um agente Sovrin, que é um software que atua como um intermediário entre o usuário e a rede. Sendo assim, o usuário pode então compartilhar seu DID a organização no qual solicita sua identidade e essa pode usar o DID para verificar as informações de identificação armazenadas na rede Sovrin. Yavuz et al. (2018) ainda diz a respeito da arquitetura da plataforma, sendo essa dividida em três camadas:

- Camada de registro: É a camada central da rede, onde são armazenadas as informações de identidade.
- Camada de agentes: É a camada que permite aos usuários interagir com a rede.
- Camada de clientes: É a camada que é usada pelos aplicativos para acessar a rede.

4. CONCLUSÃO

A identidade digital são as qualidades específicas de uma pessoa que permitem o seu reconhecimento, sendo essas informações frequentemente solicitadas em diversos sites e redes sociais para a criação de perfis. No processo de criação desses perfis, se torna comum que uma pessoa tenha múltiplas identidades na internet, essas que na maioria das situações não é possível garantir a autenticidade das informações fornecidas pelos usuários. O gerenciamento moderno de identidade e acesso está sujeito a muitas vulnerabilidades no qual envolve sistemas e hardware, apresentando um grande desafio tornar os dados pessoais seguros.

Porém, ao se aprofundar na pesquisa realizada, utilizando a metodologia de revisão integrativa focada nos temas que abrange a blockchain, gerenciamento de identidade e identidade digital, foi possível entender e conceituar essa tecnologia disruptiva, de forma a compreender como essa contribui para garantir a segurança dos dados, descentralização das informações e confiabilidade através do encadeamento de blocos e criação do livro de registro. Através da tecnologia blockchain junto a seus pilares, é possível desenvolver melhores formas de cada um ter acesso total a seus dados pessoais de forma segura, criptografada e sem passar por terceiros.

Se conclui através deste que a blockchain se abrange para vários ramos além do financeiro, e que a preocupação em transformar essa tecnologia cada vez mais popularizada, onde se pode já observar diversas ferramentas como sovrin e e-residency que mudam e traz qualidade de segurança e eficiência no uso de identidades digitais.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Paulo Henrique et al. Desmistificando blockchain: conceitos e aplicações. **Computação e Sociedade**, Sociedade Brasileira de Computação. Disponível em: <http://www-di.inf.puc-rio.br/~kalinowski/publications/AlvesLNRLK20.pdf>, 2018.

BATISTA, Alex Oliveira Abreu et al. Identificação digital baseada em blockchain: Um conceito disruptivo no ciberespaço. **Simpósio Internacional de Inovação em Mídias Interativas**, v. 5, p. 307-320, 2018.

CHICARINO, Vanessa RL et al. Uso de blockchain para privacidade e segurança na internet das coisas. **Sociedade Brasileira de Computação**, 2017.

COSTA, Bruna Stefany da. E-Estônia: digitalização dos serviços públicos da estônia. 2019.

EL HADDOUTI, Samia; EL KETTANI, M. Dafir Ech-Cherif. Analysis of identity management systems using blockchain technology. In: **2019 International Conference on Advanced Communication Technologies and Networking (CommNet)**. IEEE, 2019. p. 1-7.

FORNASIER, Mateus de Oliveira. A democracia e a tecnologia blockchain. **Sequência (Florianópolis)**, v. 42, p. e71337, 2022.

LIMA, Reynaldo Dezen et al. BLOCKCHAIN: conceito e aplicações. 2022.

LUCENA, Antônio Unias de; HENRIQUES, Marco Aurélio Amaral. Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum. **IX Encontro de Alunos e Docentes do DCA/FEEC/UNICAMP**, v. 9, p. 1-4, 2016.

MANHANI, Guilherme Augusto Rocha; DE QUEIROZ, Marc Antônio Vieira. Aplicação de Blockchain em identidades autossobranas visando cidades inteligentes. **Revista Terra & Cultura: Cadernos de Ensino e Pesquisa**, v. 36, n. 70, p. 28-36, 2020.

NAKAMOTO, Satoshi; BITCOIN, A. A peer-to-peer electronic cash system. **Bitcoin.**— URL: <https://bitcoin.org/bitcoin.pdf>, v. 4, n. 2, p. 15, 2008.

SIMMONDS, Paul. The digital identity issue. **Network Security**, v. 2015, n. 8, p. 8-13, 2015.

YAVUZ, Emre et al. Towards secure e-voting using ethereum blockchain. In: **2018 6th International Symposium on Digital Forensic and Security (ISDFS)**. IEEE, 2018. p. 1-7.