MARCOS PEREIRA NASCIMENTO

Da identidade digital à identidade digital Auto Soberana em ambiente descentralizado: um estudo da literatura e de viabilidade

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática.

Área de Concentração: Ciência da Computação

Orientador: Prof. Dr. Edson Emílio Scalabrin

CURITIBA
Fevereiro/2022

AGRADECIMENTOS

Tenho muito a agradecer. Para mim, agradecer é um exercício de reconhecer as próprias limitações humanas.

É, uma forma de reconhecer pessoas e/ou organizações que de alguma forma contribuíram para que alcançássemos sucesso diante das dificuldades encontradas durante a jornada.

Antes de tudo, sou grato a Deus, por ter me dado energia em momentos que pensei que não suportaria. Nos meus momentos de trevas, sempre via uma luz que me encorajava a prosseguir.

Maria Fernanda e Ana Laura, minhas filhas, vocês são minha inspiração para que eu começasse esse mestrado, que de alguma forma vai influenciar vocês no futuro a buscar o conhecimento.

A minha esposa Juliana sou muito grato, por ter me dado apoio nos momentos de dificuldades, que não foram poucos, e pela compreensão quando precisava me ausentar em função da escrita deste trabalho.

Ao meu pai Roque Gallo e minha mãe Irene, serei eternamente grato e ciente do esforço da parte de vocês: por me ensinar a buscar ser uma pessoa melhor todos os dias.

Sou muito grato aos colegas que fiz durante o mestrado dentro da PUC-PR, eles foram muito importante para mim no meu crescimento pessoal. Gostaria de agradecer, em especial, ao colega Eduardo Alexandre Franciscon, fiz um grande amigo, e isso não tem preço que pague, pois suas contribuições me ajudaram muito na condução do meu mestrado e por isso eu sou muito grato.

Agradeço com muito carinho as professoras Sheila Reinehr dos Santos e Andreia Malucelli, pela paciência em me conduzir pela seara da metodologia científica, o qual resultou na publicação de bons artigos.

Ao professor Edson Emílio Scalabrin um agradecimento muito especial. Pelos diversos momentos de aula, das conversas que me auxiliaram na escolha pelo tema agentes de software e durante as orientações na conclusão desta dissertação. Suas orientações foram muito preciosas para o meu crescimento profissional. Além disso, professor seu exemplo como profissional e como amigo é muito honroso, e por isso irei carregar comigo e repassar esses bons exemplos para outros alunos no futuro. Minha mais sincera gratidão professor por tudo isso.

Sumário

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

CA	*Certification Authority*
DAPPS	*Descentralized applications*
DID	*Decentralized Identifiers*
DPKI	*Decentralized Public Key Infrastructure*
GDPR	*General Data Protection Regulation*
HYPERLEDGER	*Multi-project open source collaborative*
IoT	*Internet Das Coisas*
IPFS	*InterPlanetary File System*
LGPD	*Lei Geral de Proteção de Dados (LGPD) / Lei 13.709/2018*
MAS	*Multi Agent Systems*
P2P	*Peer-to-peer*
PKI	Public Key Infrastructure
VC	*Verifiable Credentials*
W3C	*World Wide Web Consortium*

Título: Da identidade digital à identidade digital Auto Soberana em ambiente descentralizado: um estudo da literatura e de viabilidade

Resumo: *A noção de identidade, em geral, trata da relação do próprio ser com ele mesmo. Já a identidade no formato digital surge como um procedimento para o controle e a representação das informações sobre indivíduos em uma sociedade contemporânea. Logo, uma identidade digital assume a forma de um conjunto de identificadores, expressos por meio de atributos, cujas instâncias permitem distinguir uma entidade de outra. A identidade digital é um método que facilita, por exemplo a inclusão social, para dar acesso a serviços essenciais: saúde, educação, direitos eleitorais, serviços financeiros e programas de segurança social. Em termos de arquitetura esse modelo é centralizado, atribuído e outorgado por uma autoridade. No entanto, no modelo onde a identidade é local, ela é construída, gerida e usada pelo seu proprietário, mantendo a auto soberania. A identidade digital Auto Soberana pode dar as pessoas maior controle sobre a presença digital. No tempo, as arquiteturas de identidade digital evoluíram do modelo centralizado, passando pelos modelos federado e auto soberano até ao auto soberano com uso de blockchain—descentralização do controle. Esse trabalho, centrou os esforços na realização de um estudo amplo, de um lado, sobre os diferentes modelos em torno de identidade digital e auto soberana, e, de outro lado, sobre as diferentes arquiteturas de aplicações para dar suporte aos diferentes modelos de identidades. Desse estudo construiu-se um protótipo de aplicação colocando em prática o modelo de identidade digital Auto Soberana, sobre uma arquitetura baseada em estruturas de Ledger global e local—Dossiê. As tecnologias utilizadas foram: Ethereum, smart contracts, metamask, e Solidity. O resultado desse experimento permitiu mostrar a viabilidade de uso de tais tecnologias para colocar em prática um modelo de identidade digital Auto Soberana.*

Palavras-chaves: *Identidade Digital*, *Identidade Digital Auto Soberana*, *Blockchain*, *Ledger*, *Dossiê*

Title: From digital identity to self-sovereign digital identity in a decentralized environment: a literature and feasibility study

Abstract: *The notion of identity, in general, deals with the relation of the being itself with itself. The identity in the digital format appears as a procedure for the control and representation of information about individuals in a contemporary society. Therefore, a digital identity takes the form of a set of identifiers, expressed through attributes, whose instances allow distinguishing one entity from another. Digital identity is a method that facilitates, for example, social inclusion, to provide access to essential services: health, education, electoral rights, financial services, and social security programs. In terms of architecture, this model is centralized, assigned and granted by an authority. However, in the model where identity is local, it is constructed, managed, and used by its owner, maintaining self-sovereignty. Self-Sovereign digital identity can give people greater control over their digital presence. Over time, digital identity architectures have evolved from the centralized model, through the federated and self-sovereign models, to the self-sovereign using blockchain—decentralization of control. This work focused its efforts on carrying out a broad study, on the one hand, on the different models around digital and self-sovereign identity, and, on the other hand, on the different application architectures to support the different identity models. From this study, an application prototype was built, putting into practice the Auto Sovereign digital identity model, on an architecture based on global and local Ledger structures—Dossier. The technologies used were: Ethereum, smart contracts, metamask, and Solidity. The result of this experiment allowed to show the feasibility of using such technologies to put into practice a model of Auto Sovereign digital identity.*

Keywords: *Digital Identity, Self-Sovereign Digital Identity, Blockchain, Ledger, Dossier.*

INTRODUÇÃO

A evolução do mundo digital tem exigido novas soluções diante de novos desafios, dada a maior complexidade dos ecossistemas digitais existentes. Isso inclui os riscos em assegurar a privacidade de usuários em razão de crescentes ataques cibernéticos e consequentemente o indevido uso dos dados. Tais riscos afetam negativamente a reputação das empresas e a confiança dos usuários. Logo, ter a garantia de quem está acessando uma dada aplicação é o verdadeiro usuário—ou o autorizado para tal—causa preocupação tanto no mundo acadêmico quanto no mundo das organizações públicas e privadas. A questão/preocupação está em assegurar um nível de confiabilidade significativo nas aplicações, buscando, portanto, garantir um ambiente confiável, em especial nas comunicações/trocas tanto no longo prazo quanto no curto prazo. A questão central é garantir a proteção de dados e a identidade do proprietário, ou dos autorizados para uso, bem como assegurar a soberania do usuário no compartilhamento de tais dados.

1.1 Descrição do Problema

Muito do que chamamos de "identidade" pode não ser uma identidade se visto sob o olhar filosófico, no máximo, é um conjunto de identificadores. Em MAIA (2008), do ponto de vista mais filosófico, a noção de identidade encerra uma construção que ocorre em conjunto com uma reflexão sobre o conceito de *ser*. Por outro lado, sob a ótica da abordagem sistêmica das organizações, em SCAICO (1985) a noção de identidade tem alcance menos abrangente e mais restritiva, já que é especificada por meio de componentes em um sistema, expressa por meio de determinados atributos e/ou identificadores, cuja combinação peculiar distingue esses componentes dos demais e confere uma identidade no sistema.

Identificadores ou diferenciais são os elementos que uma organização reconhece você; você como um cidadão, você como um motorista, você como um estudante, e assim por diante. Essas organizações podem atribuir um número sequencial ou não, na forma de um passaporte, licença ou cartão de membro. Contudo, isso pode não ser uma identidade, no máximo será um identificador. Na relação dos identificadores, para MORELLATO (2021) a afirmação recai sobre informações extraídas de dados coletados que identifiquem ou que tornem identificável uma pessoa natural/física, o conceito inclui, por exemplo o nome, RG,

CPF e endereço, entre outros.

No cenário estudado, identidade representa um subconjunto de elementos abertos que representem o indivíduo face a um contexto específico. Aqui o conceito de identidade como um número tem serventia limitada. Por exemplo, não é suficiente apresentar o seu número de CPF ou RG para contratar um empréstimo em uma instituição financeiro. O CPF não é suficiente para definir quem você é para a instituição financeira; ou seja, um conjunto de outros indicadores vão ser necessários para compor a sua identidade—e comunicar quem você é para a instituição financeira—, como por exemplo, os bens, direitos, competências, etc.

Em CASTELL (2018), reforça-se a ideia que é necessário estabelecer uma distinção entre a identidade e os papéis que os indivíduos assumem, a partir de normas estruturadas pelas instituições na sociedade. Em outras palavras, entende-se identidade como o indivíduo é reconhecido por si mesmo. Essa abordagem, nos permite acreditar que há elementos "mais pessoais" de natureza física, econômica e social sobre controle exclusivo do sujeito, os quais fortalecem a criação da própria identidade. Essa *capacidade exclusiva* de ter o controle sobre os próprios elementos pessoais—de si mesmo—denomina-se *capacidade auto soberana* (PREUKSCHAT, 2021). A partir desse ponto, pode-se falar da identidade como sendo o conjunto de atributos dinâmicos controlados pelo próprio sujeito. É dinâmico, pois os atributos mudam no tempo, por exemplo, ter concluído um curso superior é uma mudança nas características que representam esse mesmo indivíduo.

Há, portanto, um problema a ser resolvido em relação aos modelos de identidade, já que na maioria dos casos, quem controla ou quem atribui um identificador ao usuário é uma entidade externa, detentora da fé-pública para conceder uma identidade válida—um identificador—perante as organizações. Em SOLOVE (2005), as organizações criam uma pasta digital sobre os indivíduos, a qual será alimentada pelos fluxos de informações ligados pelos negócios, organizações e entidades governamentais. O fluxo de dados refere-se a maneira de descrever como os dados se movimentam entre as grandes bases de dados do setor privado, dos registros públicos e pelos agentes da lei.

Nesse cenário, como também apresentado em STOKKINK (2018), NAIK *et.al.* (2020) e AHMED *et. al.* (2020), existe a necessidade de quebrar o *paradigma de identidade centralizada*, denominado de *terceira-parte*, para um novo *paradigma descentralizado* e *controlado exclusivamente pelo próprio usuário*. O *paradigma*/*ambiente* a ser percorrido será o digital, e nesse universo os indivíduos podem ser vistos como agentes virtuais ou computacionais, ou um *snapshot* caracterizado como sendo uma cópia de si mesmo. Em outras palavras, uma *virtualização* no espaço, contento todo o *histórico de vida* que represente

aquela pessoa/indivíduo; é um *metaverso*[1]*, ou seja,* o espaço compartilhado que tentará replicar a realidade. Em CASTELL (2005) as pessoas, na sua maioria, não escondem a sua identidade na *Internet*, exceto algumas de pessoas que buscam o *anonimato* em função do contexto de vida. Atualmente, as pessoas estão integrando as tecnologias nas suas vidas, ligando a realidade virtual com a virtualidade real, vivenciando várias formas tecnológicas de comunicação, articulando-as conforme as suas necessidades.

Do ponto de vista da computação, busca-se resolver a questão da identidade digital controlada pelo indivíduo, que encerram algumas etapas a serem vencidas, em especial como *garantir* ao próprio usuário o *controle* e o *consentimento* de *uso* sobre as próprias informações na utilização de *identificadores* e, ainda como assegurar a existência de uma fonte de dados confiável, de tal forma imutável que certifique que as informações apresentadas pelos indivíduos sejam verdadeiras. No campo da Ciência da Computação, para a etapa do controle das próprias informações do ponto de vista do indivíduo, há o modelo de *identidade digital Auto Soberana*, e, em relação a estrutura de dados que permite manter uma fonte local de dados fidedigna, pode-se citar o uso da tecnologia blockchain e do modelo *Dossiê* criado por SILVA (2017).

O problema é: envolvendo um usuário no ambiente digital, como assegurar, de forma descentralizada, a sua identidade digital auto soberana?

Os elementos—identidade digital, Identidade Digital Auto Soberana, blockchain e *Dossiê*—são objetos/conceitos distintos propostos em contextos diferentes, no entanto, quando tomados em conjunto permitem vislumbrar uma arquitetura que pode contribuir para resolver o problema em questão. Em outras palavras, o desafio é fazer com que as propostas —*Identidade Digital Auto Soberana*, blockchain e *Dossiê*—caminhem juntas em um *ambiente descentralizado.* Dessa forma, ao longo dessa dissertação, busca-se, entender o que deve ser colocado em prática para garantir a *imutabilidade de dados sensíveis* no *compartilhamento ativo* de informações pessoais, de históricos de atividades, de diretos de posse de bens, no acesso a serviços públicos e nas transações financeiras entre usuários.

Aqui, assume-se que há uma *estrutura de dados* que *comporta* os *históricos de vida* dos usuários. Essa estrutura, em um dado *contexto* representa o *conjunto de atributos* que

[1]https://pt.wikipedia.org/wiki/Metaverso

compõe a identidade do indivíduo. Entende-se como *contexto* a circunstância onde o agente/usuário é parte ativa, e a identidade do agente/usuário pode ser composta seletivamente pelos atributos que fazem sentido no contexto corrente. Deve-se entender o termo agente como uma entidade de software que realiza objetivos próprios e/ou de terceiros (ex. um ser humano); e para facilitar a descrição das interações entre agentes, esses últimos podem assumir papéis distintos (e.g. comprador/cliente, vendedor/servidor/provedor). Por exemplo, se um *agente—comprador*—está em processo de compra de um veículo de outro *agente—vendedor*—, as informações necessárias para a realização da transação de compra são parcialmente diferentes ou totalmente diferente daquela, por exemplo, se o *agente—comprador*—estiver em uma transação envolvendo um *agente* do Governo—Receita Federal—na aquisição de um bem importado.

Assume-se, também que cada transação é um contrato no que tange aos direitos e às obrigações de cada parte, e como não há terceirização de direitos e de obrigações, os dados e o controle são geridos localmente—a exemplo do modelo *Dossiê* criado por SILVA (2017). Esse último quando construído dentro de uma arquitetura blockchain visa assegurar a imutabilidade e a localidade dos dados no próprio agente. Por outro lado, em relação a privacidade dos dados busca-se garantir restrições de publicidade ou de acesso sem *consentimento* do seu proprietário, já que permitir acesso parcial/controlado de informações, por exemplo, classificadas em um dossiê, requer a seleção dos dados a serem compartilhados. Essa arquitetura se apropria do modelo *Dossiê,* mas não de forma *ipsis litteris*, face a proposta original não comportar o compartilhamento seletivo de informações.

O outro assunto subjacente a nossa pesquisa concerne a *violação de privacidade, que* é cada vez mais comum no ambiente digital, o que pode comprometer severamente a segurança de uma aplicação, expondo, por exemplo, dados pessoais por meio de acesso não autorizado de sistemas de informações. Para ZYSKIND (2015), o crescente aumento de incidentes dessa natureza faz-se questionar se o modelo atual—onde *provedores terceirizados* tem *o controle* sobre grande quantidade de informações dos usuários—é realmente *eficaz.* Essa ideia foi *reforçada em* SOLTANI (2018), em que o modelo do *gerenciamento de informações de usuários* mais aceito pela maioria das organizações é aquele *centralizado* no próprio provedor, ou no provedor que recebe a *outorga* para permitir acesso aos dados. Deve-se, no entanto, garantir a segurança com vistas a assegurar a privacidade dos dados dos usuários contra acessos indesejáveis ou a exposições indevidas.

Para FREUND (2018), a centralização foi e ainda é um conceito importante em nosso desenvolvimento social, em função dos benefícios originados de uma sociedade centralizada,

conectada por meio de dados, permitindo a criação de serviços e de inovações, as quais têm promovido a geração de riquezas e de transformação social. No entanto, há a preocupação em relação a privacidade dos usuários. Essa preocupação está relacionada ao fato de que a grande maioria dos dados/riquezas estão centralizados exageradamente em organizações as quais acumulam quantidades significativas de informações pessoais e sensíveis de seus usuários.

Em SOLTANI (2018), o modelo atual de gerenciamento de dados dos usuários atende apenas as necessidades dos provedores de serviços e não dos proprietários ou dos usuários dono da informação. De certa forma, uma consequência imediata de tal modelo é que, se o usuário não for aceito por aquele provedor de serviços cuja chancela é atribuir confiança ao indivíduo, esse indivíduo é excluído de todos os benefícios que outros já desfrutam, pois estão "dentro" e aceitos pelo sistema—ou provedor de serviços. Porém, tal sistema não é binário, mas tem muitas camadas de confiança e, portanto, quanto mais confiável alguém é, mais benefícios ele desfruta, como exemplo: ter conta bancária, carteira de motorista, escritura do imóvel, empréstimos para comprar um carro novo. Isso corrobora com a ideia de que o acesso a informações exclusivas dá vantagens econômicas individuais. Uma consideração a ser fazer é que os sistemas de informações recebem credenciais de confiança emitida por seres humanos, embora eles sejam falíveis e corruptíveis.

Para FREUND (2018), quanto mais tem-se acesso à informação, mais pode-se influenciar nas decisões de agentes de confiança—ou de certificação—em relação a benefícios próprios ou de grupos. O inverso, portanto, também é verdadeiro, levando, por exemplo, à exclusão financeira. Para o usuário incluso—ou aceito—no Sistema, sua credencial é validada, acreditada dentro do modelo, o qual atribui a ele fé pública, gerando confiança e reputação. Em consequência, o usuário aceito é inserido em uma categoria e a ele é atribuído um *score*, o qual permite aos *provedores de dados* e de *serviços* gerenciar a vida digital desse indivíduo. Logo, se por um lado o acesso aos serviços de informações possibilitou aos provedores de serviços categorizar os usuários—identifica-os por meio de chaves ou códigos dentro de um modelo de centralizado de identidades—, por outro deixou de fora ou excluiu dos sistemas aqueles que não podem ou não têm meios de criar uma identidade digital.

Em MA *et. al*. (2018), o próprio Banco Mundial tem endossado a premissa de que a inclusão financeira dos "não-bancarizados" pode ocorrer por meio de uma prova válida de identidade. Uma identidade digital válida é um importante método para a inclusão socioeconômica, para dar acesso a serviços essenciais, como saúde e educação, direitos eleitorais, serviços financeiros e aos programas de segurança social. O instrumento da

identidade digital fortalece a administração eficaz e eficiente de serviços públicos, permitindo decisões políticas transparentes e governança aprimorada, especialmente para reduzir a duplicação e o desperdício.

Desse modo, o acesso a informações precisas, com a preservação da privacidade e da segurança das informações são essenciais no controle de identidades. Nesse sentido, ter controles efetivos para garantir a privacidade de modo adequado, resguardar a visibilidade das informações quando compartilhados por terceiros é fundamental. Esses problemas tornaram-se recentemente mais visíveis em parte devido a novos regulamentos, tais como a *Lei Geral de Proteção de Dados (LGPD) — Lei 13.709/2018.* Por fim, em STOKKINK (2018), uma possível solução decorre da adoção de um modelo de identidade digital que não necessite ser validado por uma *terceira parte*. A identidade é local e descentralizada, construída, gerenciada e usada pelo usuário proprietário das informações. O proprietário da identidade não está mais vinculado a uma única *autoridade central*. Em tal modelo, as empresas e instituições não precisam mais confiar umas nas outras, **eles precisarão confiar no usuário.**

1.2 Objetivos

Tendo em vista que a grande maioria dos modelos de identidades digitais estão baseados na centralização das informações, pois o *agente provedor* ou a *terceira-parte* é a parte com o poder de atribuir *confiança* e *reputação* ao usuário, nesse trabalho, visa-se estudar a viabilidade de um modelo de identidade digital onde o próprio usuário tem o controle das próprias informações para serem compartilhadas, quando o usuário atua em ambientes descentralizados. O modelo estudado busca evidenciar a viabilidade técnica denominada de *identidade digital Auto Soberana*.

Para a consecução do objetivo acima foram definidos os seguintes objetivos específicos:

1. Realizar estudo do estado da arte em relação as iniciativas em torno dos modelos de identidades digitais.
2. Realizar estudo do estado da arte em relação ao uso da tecnologia *blockchain* face a infraestrutura para a implantação de modelos de identidades digitais descentralizadas.
3. Propor um modelo de identidade digital, cujo controle das informações é outorgado ao usuário, denominado de *Identidade Digital Auto Soberana*.

4. Desenvolver um protótipo para colocar em evidência as práticas e os conceitos em torno do modelo de identidade digital Auto Soberana, com uma arquitetura descentralizada, usando cadeias de blocos—*blockchain*.

1.3 Contribuições

A principal contribuição desse trabalho foi apresentar um modelo de identidade digital, cujo controle das informações é outorgado ao usuário, denominado de *Identidade Digital Auto Soberana*. Para compor essa identidade com intuito de assegurar informações fidedignas foi estabelecida uma fonte exclusiva de informação que provém de uma estrutura local—o *Dossiê* de cada parte/agente. Essa estrutura local de dados foi adequada para suportar a seletividade de informações, cuja opção não fazia parte da ideia original do Dossiê. A proposta foi posta em execução, em ambiente simulado com o objetivo de ilustrar a criação de identidade *Auto Soberana* de um agente originada pelas informações fornecidas pela estrutura/arquitetura local de cada agente. As informações relativas as interações entre os agentes foram realizadas por meio de transações inseridas dentro da cadeia da blocos da *Ethereum* utilizando-se de uma carteira digital. Uma outra contribuição está na condução de uma revisão sistemática da literatura, empreendida no início da pesquisa, em especial para o aprofundamento dos modelos de identidades digitais no contexto de privacidade da informação e arquiteturas blockchain.

1.4 Estrutura do Documento

Esta pesquisa está organizada em *7 capítulos*. O primeiro *Capítulo 1* apresenta uma breve introdução e os objetivos do trabalho. O *Capítulo 2* contém a fundamentação teórica sobre identidades digitais e modelos de identidade digital. No *Capítulo 3* é apresentado o *modelo da identidade Auto Soberano* e as respectivas características que compõe tal modelo. Em seguida no *Capítulo 4* é apresentado os conceitos de Identidade Auto Soberana aplicado no contexto de *blockchain*. No *Capítulo 5* detalha-se a aplicação da estrutura *Dossiê* em conjunto com o modelo *Auto Soberano* nas estruturas de *ledgers distribuídos*. No *Capítulo 6* ilustra-se a aplicação do modelo de identidade Auto Soberana em conjunto com a tecnologia *blockchain*. Por fim, o *Capítulo 7* encerra com uma discussão, conclusões e possíveis futuros trabalhos.

2 Identidades Digitais

2.1 Introdução

Este capítulo apresenta os referenciais teóricos básicos relacionados a esta pesquisa. Neste contexto serão apresentados conceitos sobre *privacidade* do usuário, vistos sobre os olhares conceitual e *computacional* do termo, abordando as relações, definições gerais, características e protocolos das aplicações. Em seguida, será apresentado o conceito sobre *identidade digital* e os principais modelos existentes, em especial, dar-se-á ênfase ao modelo de identidade digital *Auto Soberano*, examinando as suas características.

Esses conceitos são importantes para o entendimento deste trabalho. O que se procura é entender e elucidar: a relação entre a gestão local dos dados—mantida, por exemplo, por um agente de software—e o compartilhamento desses dados. Para tanto, assume-se aqui, como premissa básica, que os dados e o controle de uma aplicação são distribuídos logicamente e/ou fisicamente a luz do modelo canônico de um sistema de agentes de software, em que se busca favorecer a comunicação e a gestão local de dados; em particular, a veracidade desses dados e a sua privacidade.

2.2 A privacidade do ponto de vista conceitual e computacional

Uma das inquietações do mundo moderno/digital, presente no quotidiano das pessoas, diz respeito a questões em torno da *privacidade* digital. Em ARORA (2019), à medida que o compartilhamento de informações se torna mais onipresente, o conceito sobre a privacidade atraí muito mais atenção. As iniciativas de *transparência* e de *controle* da privacidade, com base no regime de *consentimento*, têm sido apontadas como importantes medidas para ajudar os indivíduos lidarem com a privacidade dos dados.

CHO (2019) enfatiza que as pessoas estão preocupadas—ou cientes—com os riscos de privacidade. Na medida em *informações pessoais* quando, por exemplo, disponíveis de modo online/digital podem ser facilmente coletadas, compartilhadas e, eventualmente, serem mal utilizadas por terceiros, incluindo empresas, governos e até mesmo seus próprios amigos. Neste contexto de exposição ao mundo digital, a privacidade da informação é um fator chave que pode influenciar o comportamento de cada usuário do ambiente digital.

Na *Tabela 1* é apresentado os conceitos sobre privacidade encontrados na literatura do ponto de vista *conceitual* e *computacional*.

Tabela 1. O conceito de privacidade do ponto de vista conceitual e computacional.
A presença da característica (✓) ou a ausência (●). Adaptada de LIU et. al. (2020)

Trabalho	**Conceito de privacidade**	**Acesso remoto de dados**	**Anonimato**	**Confidencialidade dos dados**	**Controle no usuário**
VIKRAM et. al. (2021)	✓	●	✓	✓	●
CHEN et. al (2021)	✓	●	●	✓	●
WEINHARDT (2021)	✓	●	●	✓	●
RUDDELL et. al. (2020)	✓	✓	●	✓	●
DURNELL et. al. (2020)	✓	●	✓	✓	●
SMOLAK et. al. (2020)	✓	●	✓	✓	●
LESAVRE et. al. (2019)	✓	●	✓	●	✓
KASSEM et al. (2019)	✓	●	●	●	✓
REN et. al. (2019)	●	✓	●	✓	●
MELL et. al. (2019)	●	●	✓	●	✓
HAMER et. al. (2019)	✓	✓	✓	●	✓
HANG et. al. (2019)	✓	●	●	✓	●
WILLIAMS et al. (2019)	✓	●	●	●	●
BECKER (2019)	✓	●	●	●	●
FABER et al. (2019)	●	✓	✓	●	●
JAMAL et al. (2019)	●	✓	●	●	✓
FAN et al. (2019)	●	✓	✓	●	●
LEE et al. (2019)	●	●	✓	✓	✓
HOEL et al. (2018)	●	●	●	●	●
GRÜNER et al. (2018)	●	✓	●	●	✓
ABRAHAM et al. (2018)	●	●	●	✓	✓
OTHMAN et al. (2018)	✓	✓	●	●	✓
SOLTANI et al (2018)	●	●	✓	✓	●
STOKKINK et al. (2018)	✓	●	●	✓	✓
MIKULA et al. (2018)	●	●	✓	●	●
TAKEMIYA et al. (2018)	●	✓	●	●	●
SCHANZENBACH et al. (2018)	●	✓	●	●	✓
BAARS et al. (2016)	●	●	✓	✓	✓
BASTIAN (2015)	✓	✓	●	●	✓
AGUIRRE et.al (2015)	●	✓	●	✓	●
CAO et al. (2010)	✓	●	✓	●	✓

Neste contexto, das *diferentes acepções* sobre o que é a *privacidade* apresentadas na *Tabela 1*, PAINE *et. al*. (2007), ainda reforçam que a privacidade pode ser vista e compreendida por meio de *dimensões*: a capacidade de controlar e limitar a *interação física* no *acesso psicológico* e *informativo* da informação sobre si mesmo ou de um grupo. Assim, se a privacidade é vista como uma *construção unidimensional*, o foco da dimensão é apenas da *privacidade informacional.* No entanto, por natureza, a privacidade é *multidimensional*, já

que ela envolve aspectos *físicos, psicológicos* de uma *interação verbal e não-verbal*. A conceituação de privacidade é complexa e sua falta de precisão reflete nas preocupações crescentes das pessoas e das organizações, onde são, por exemplo, criadas normas e/ou leis específicas para tentar acomodar inquietações legítimas, em particular, no contexto do ambiente digital.

2.3 Privacidade dos dados pessoais

Há uma confusão sobre o que realmente são *dados* e o que é *informação*. Em AL-KHOURI (2012) a verdade é que os dados não são mais do que um conjunto de caracteres que, se não forem vistos em um dado *contexto*, são desprovidos significado. Dados são o que se usa para fornecer algumas informações. Logo, o contexto e o uso fornecem um significado aos dados, os quais geram ou constituem informações. Assim, os dados na forma bruta não encerram relevância e, portanto, nenhum valor. Quando não há valor nos dados, pode-se supor que a propriedade não é um problema.

Por outro lado, em HARDJONO *et.al* (2019) os dados digitais são criados por e sobre pessoas e estes podem gerar novas ondas de oportunidades para a criação de valores econômicos e sociais. Os tipos, quantidades e valores de dados pessoais são vastos. Nesta linha, pode-se destacar: perfis em aplicativos, dados demográficos, contas bancárias e registros médicos. Como também, dados das pesquisas realizadas na web ou de sites visitados: incluindo gostos e desgostos e os históricos de compras. Essa lista de destaques deve continuar crescendo nos próximos anos.

As empresas coletam e usam esses dados para apoiar a entrega individualizada de serviços em modelos de negócios monetizados. Os governos empregam dados pessoais para fornecer serviços públicos críticos de forma mais eficiente e eficazes. Os pesquisadores empregam grandes massas de dados para acelerar o desenvolvimento de novos medicamentos e de protocolos de tratamento. Já os usuários finais, se beneficiam de recursos gratuitos normalmente personalizados com vistas a gerar melhor experiência para o consumidor, como por exemplo, nas pesquisas web, redes sociais ou em sites de comprar—recomendação de produtos ou de serviços.

WIERINGA *et.al.* (2019), ambientes ricos em dados digitais fornecem para pesquisadores e/ou fabricantes de produtos oportunidades únicas para obter detalhes e percepções sobre o comportamento e opiniões dos clientes. Estes conjuntos de dados são, muitas vezes, chamados de *big data*, caracterizados principalmente pelo alto volume e/ou

diversidade de dados.

No entanto, é notado que à medida que se evolui na era digital, novos riscos surgem em relação à privacidade do indivíduo. Nesse cenário, SMITH *et.al.* (1996) entendem a privacidade dos dados como a capacidade do indivíduo controlar pessoalmente as informações sobre si mesmo. Compreendendo o conjunto de registros de dados pessoais que, ao ser acessado, sem autorização, causa prejuízo sobre vários aspectos da vida do indivíduo. Na verdade, falar em risco de privacidade é falar em *exposição em potencial*, *acesso não autorizado* ou *perda do controle* sobre os dados pessoais. Parar MILBERG *et.al.* (1995) a questão implica em valores éticos a serem observados pelos gestores, sendo um *trade-off* entre operação eficiente e eficaz para as empresas e a proteção das informações pessoais.

Em outro cenário, não há a exposição de dados dos indivíduos, mas serviços cujo modelos de negócios são construídos por meio da geração de publicidade, em que se permite os provedores de serviços web capturar grandes quantidades de informações privadas. Nesse modelo, os provedores de serviços coletam grandes volumes de informações dos usuários como forma de sustentar a centralização da informação e obter benefícios significativos por meio da descoberta de padrões de comportamento.

Dessa forma, garantir a privacidade não é apenas esconder informação do outro, ou seja, deve-se também permitir ao indivíduo direito sobre o controle de quem tem acesso a ela. A privacidade, em geral, é um direito humano de ordem constitucional. E de certo modo, esta razão já é suficiente para que o bem em torno da privacidade do indivíduo seja protegido, já que há valor intrínseco em si mesmo. Adicionalmente, a privacidade dos dados nos protege das más intenções e incompetências de outros. Em situação extrema, se o indivíduo tem certeza de que um provedor de serviços—no qual ele confiou alguns de seus mais importantes dados—, não merecem mais essa confiança, então a melhor atitude a se tomar, é revogar o acesso, fechando de pronto a exposição ao risco.

Dito de outra maneira, por exemplo, ter os históricos de gastos ou de saldo bancário expostos ao mundo não é um risco que alguém queira ter, pois dessa forma não terá qualquer controle sobre essa situação. O cenário ideal em torno do "mercado de dados", com a garantia que seja um mercado justo, é aquele onde indivíduos têm poderes sobre os dados que encerram suas transações. Para isso, requer-se não apenas estudos sobre privacidade, mas melhores práticas e meios de implementá-las.

2.4 Paradigmas de Identidades Digitais

A digitalização da economia tem promovido novos serviços e produtos aos indivíduos, os quais têm permitido a geração de riqueza e a melhoria da qualidade de vida. Nesse sentido, há uma clara evolução da vida digital, em função da criação de facilidades das aplicações que permeiam o nosso dia a dia. Para entendimento de tais mudanças, nessa seção são apresentados os elementos fundamentais em torno de o conceito sobre *identidade digital*. Em seguida, apresentar-se-á os tipos de identidades digitais e as respectivas características que as distinguem.

2.4.1 Identidade Digital

A *identidade digital* surge como um importante método para o controle de informações sobre indivíduos *vis-à-vis* a uma sociedade digitalizada—ou a caminho da digitalização. Em um determinado contexto, pode-se ter identidades digitais em relação, por exemplo, ao local de trabalho, a vida pessoal ou face as atividades profissionais. Nesse sentido, o cenário aponta para a necessidade de confiar na entidade que tem o papel de gerenciar as informações das identidades, protegendo as informações dos indivíduos, como também no fornecimento de serviços relevantes.

Para DER (2017), a *identidade digital* é uma *cópia*, um *snapshot*, um retrato instantâneo da identidade real de pessoas, empresas ou de dispositivos— de forma mais geral: de uma *entidade*. A identidade real engloba todas as características determinantes de uma entidade, o que torna uma entidade distinguível dos outros. Cada identidade digital consiste em apenas um fragmento da identidade e geralmente é criada para um propósito específico em um contexto específico: usar um serviço específico ou interagir com outra entidade.

De modo similar, para o WORLD BANK (2017), a ideia de *identidade digital* se baseia na *representação* de uma entidade em um contexto específico. Representa a *coleção de atributos* capturados e armazenados exclusivamente de modo eletrônico, com a finalidade de descrever uma pessoa dentro de um *contexto*. De modo tradicional, o conceito de *identidade digital* se associa ao da vida real, indicando atributos do tipo: quem somos, gostos pessoais ou se somos honestos ou não.

Visto de outra forma, trata-se de uma extensão do documento de identificação físico aplicado ao mundo digital. EL MALIKI *et.al.* (2013) dizem que nem sempre a relação entre a identidade física está fortemente relacionada a *identidade digital*, especialmente nos casos em que envolve serviços *online*. Por exemplo, em sistemas de

marketplace, a relação entre compradores e vendedores se consolida quase que exclusivamente na *reputação* das partes envolvidas na transação e não nos atributos dos agentes envolvidos.

É conhecido que o fortalecimento dos serviços *online* promove a conectividade onipresente na sociedade que por sua vez, também possibilita o surgimento de problemas tais como: o uso de *phishing*, *spam* e roubo de identidade. Todos esses problemas foram agravados de alguma forma pela constante mobilidade do usuário na busca e criação de relações *online*. Há, portanto, uma necessidade de enfrentar o problema de como determinar a identidade do interlocutor com a devida precisão face, em particular, as reivindicações demandas nos contextos das relações sociais, mediadas pela digitalização.

Por outro lado, é fato que apenas pelo uso das atuais formas de autenticações nos sistemas, ainda que se utilizem de recursos robustos, não tem sido suficiente para garantir a segurança nas aplicações. A proposta de *identidade digital* ganha força no intuito de garantir que não apenas as expectativas de serviço e funcionalidade sejam atendidas, mas também que se fortaleça a segurança e a privacidade dos dados.

2.4.2 Sistemas de Identidades Digitais

A *identidade digital* como apenas registros de atributos, por si só, não fornece muitas funcionalidades, pois para isso ela já conta com métodos para criar e gerenciar uma *identidade digital*. Há sistemas específicos cuja finalidade é promover a criação e o gerenciamento de identidades digitais de usuários. Esses sistemas podem ser distinguidos em função dos modelos, das arquiteturas e da finalidade.

Em YUAN *et. al.* (2010), os sistemas de identidades digitais estabelecem a comunicação, o controle de acesso, a transparência segura de atributos de identidade. Eles gerenciam não apenas o ciclo de vida da identidade, como também administram o fluxo de trabalho durante a troca de identidade entre diferentes domínios e delegações de confiança dinâmicas. A estrutura da *identidade digital* integra muitas tecnologias utilizadas para o gerenciamento e controle de acesso as informações sobre os usuários. Essa estrutura encerra políticas, regras, métodos e sistemas que implementam a autenticação da identidade para autorização, controle de acesso e operação de auditoria com base na *identidade digital*.

Por outro lado, em El MALIKI *et.al*. (2013) a identidade digital é o processo de representar, usar, manter, prover e autenticar entidades em redes de computadores. Como tal, os modelos existentes refletem a criação de sistemas cuja funcionalidade é gerenciar as

identidades digitais. As estruturas necessárias que descrevem o modelo de um sistema de identidade digital [YUAN *et. al.* (2010) e WORLD BANK (2017)], pode ser visto na *Figura 1*.

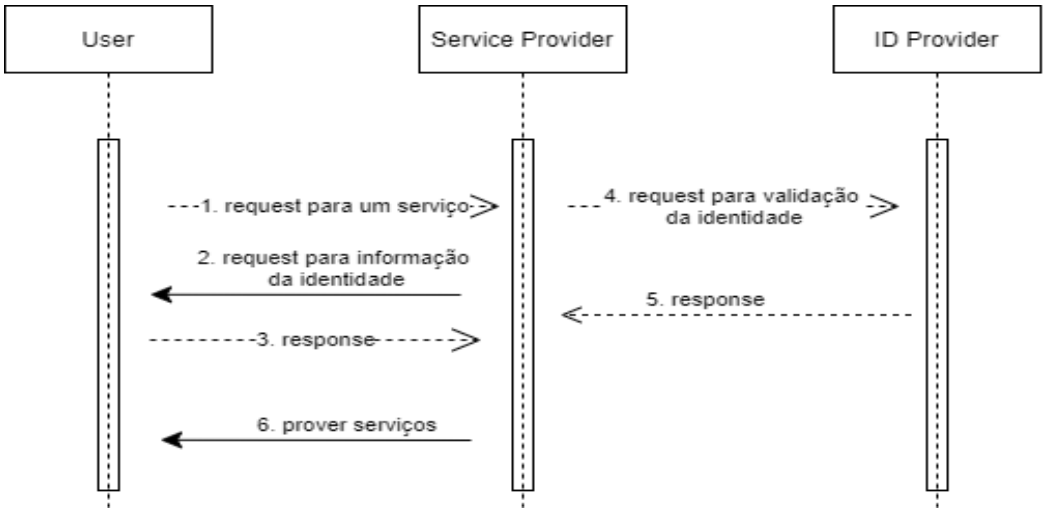

Figura 1. Ciclo de vida da identidade digital. Adaptado de YUAN et. al. (2010) e WORLD BANK (2016)

A *Figura 1* representa a arquitetura típica de um sistema de gerenciamento de *identidade digital*, cujo elementos seguem de acordo com os fundamentos apresentados em YUAN *et. al*. (2010), WORLD BANK (2017), STEVENS (2018), BOUWENS (2020) e LIU *et. al.* (2020) cujos atributos foram descritos na *Tabela 2:*

Tabela 2. Elementos que compõem a arquitetura de *identidade digital*.

Estrutura	Conceito
User	Representa os principais facilitadores do sistema, aproveita-se dos vários serviços oferecidos pelos provedores de serviços e pelos provedores de identidade. Nem todos os usuários têm o mesmo nível de privilégio.
Service provider (SPs)	Entidade que impõe uma verificação de identidade, responsável também por fornecer serviços aos usuários, quando eles são autenticados com sucesso.
Identity provider (IdPs)	Entidade que emite a identidade do usuário. O núcleo do sistema é encarregado de fornecer aos usuários serviços de identidade (e.g., registro, autenticação e gerenciamento). Esta entidade também fornece autenticação de usuário.
Identity	São objetos físicos ou lógicos com existências distintas, que incluem indivíduos e entidades coletivas (e.g., empresas, governos, bancos).
Identifier	É um atributo cujo valor pode ser usado para identificar univocamente uma entidade dentro de um contexto. Os valores descrevem: o que tem um usuário, o que é um usuário, o que sabe um usuário ou o que faz um usuário.

Para STEVENS (2018), o ciclo de vida da *identidade digital* começa com o registro do proprietário por meio de um provedor de identidade. O registro consiste na inscrição e validação de dados. Na inscrição, os principais atributos de identidade—passaporte ou

certidão de nascimento, dados biométricos, perfis sociais, etc.—são registrados e essas informações encerram implicações relativas à confiabilidade e interoperabilidade com outros sistemas de identidade.

A validação de uma identidade digital é a verificação/*matching* dos atributos fornecidos pelo proprietário da identidade com os dados existentes no provedor de atributos, por exemplo, em bases de dados biométricas ou de outros sistemas de identidade nacionais; após essa validação a *identidade digital* é instituída. A autenticação é sobre o proprietário da identidade. Ele detém o controle sobre o *identificador digital*, na medida em que ele pode usar as credenciais para ter acesso as facilidades fornecidas pelos provedores de serviços. A representação do fluxo de criação, validação e autenticação de uma *identidade digital* pode ser vista na *Figura 2*.

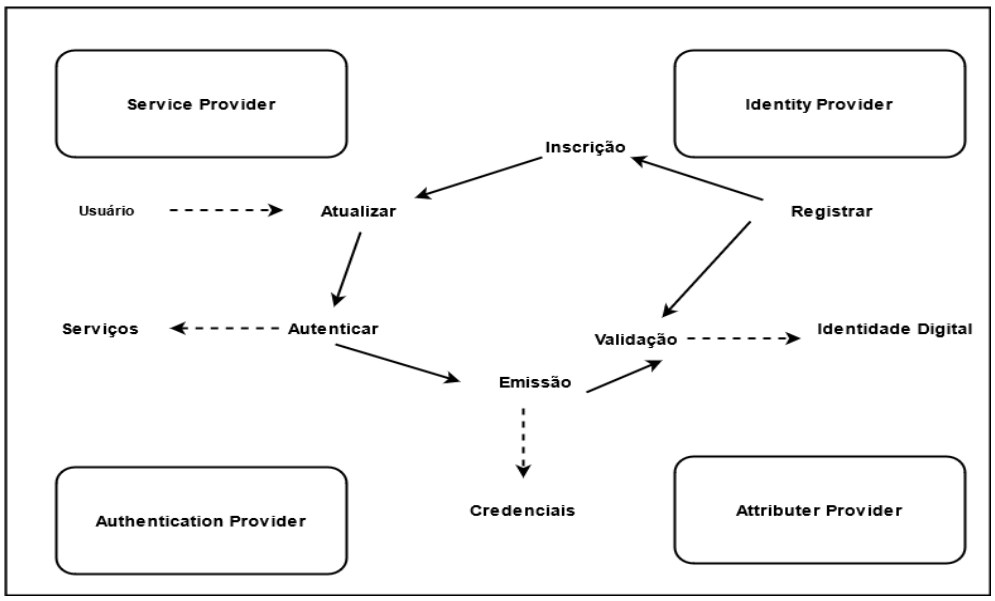

Figura 2. Representação da criação, emissão, autenticação e validação de uma identidade digital.Adaptado de KASSEN et. al. 2019

Por outro lado, cf. a *Figura 3*, uma entidade, constituída por um usuário, pode ter várias identidades, e cada identidade pode consistir em muitos outros atributos com identificadores exclusivos ou não-exclusivos.

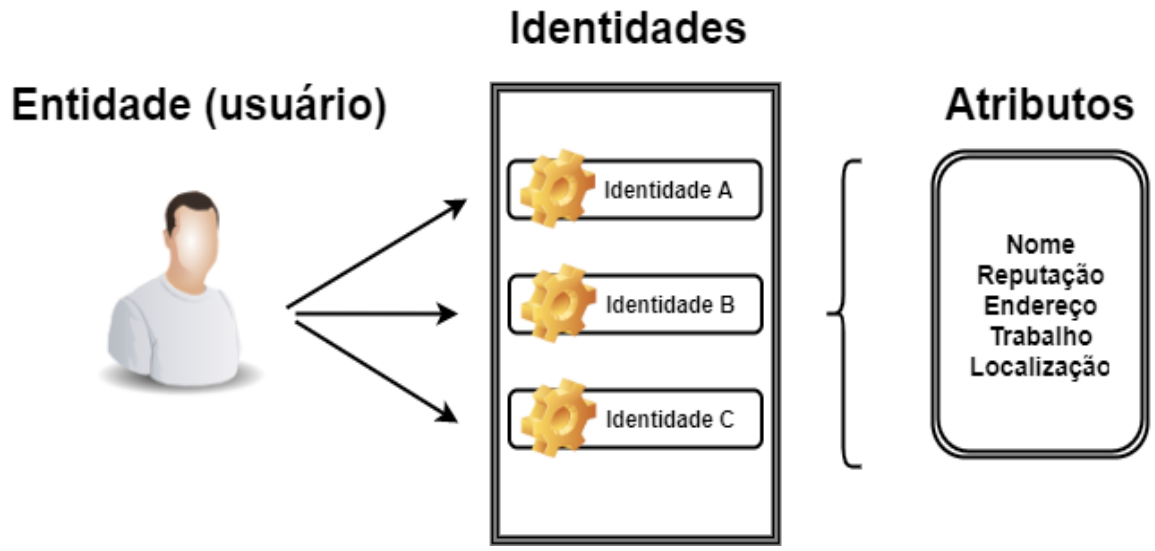

Figura 3. Relação entre identidades, atributos e entidade. Adaptado de MALIKI et.al. (2013)

Dessa forma, os modelos de identidade digital foram elaborados para lidar com as seguintes questões, em EL MALIKI *et.al.* (2013):

I. *Reduzir acesso indevido*: acessos indevidos de identidade está se tornando um grande problema, em especial no ambiente online. Os provedores precisam de sistemas mais eficientes para resolver este problema.

II. *Gerenciar identidade*: a quantidade de identidades digitais por pessoa está aumentando, diante desse cenário os usuários precisam de suporte conveniente para gerenciar essas identidades e as correspondentes autenticações.

III. *Gerenciar acessibilidade*: o gerenciamento de acessibilidade permite ao usuário lidar com seus contatos para evitar o uso indevido ou chamadas não solicitadas.

IV. *Autenticar usuário*: a garantia de integridade de acesso pode impedir o roubo de identidade.

V. *Garantir anonimato*: o fornecimento de anonimato para impedir o rastreamento ou identificação de usuários de um serviço.

2.5 Modelos de *Identidade Digital*

A *identidade digital* é um dos maiores desafios no ciberespaço. Este campo vem evoluindo em função dos diversos modelos de identidade digitais existentes, os quais estão sendo empregados em contextos diversos. No entanto, poucos modelos foram capazes de resolver a questão de *soberania*, e do controle de dados pessoais e confidenciais. Há, portanto, diferentes modelos de identidades digitais e o uso de um modelo em detrimento do outro se justifica no

seu propósito, o qual a organização pretende aplicar.

Em NAIK *et.al.* (2020) e AHMED *et. al.* (2020), os principais modelos de identidade digital podem ser vistos na *Figura 4*:

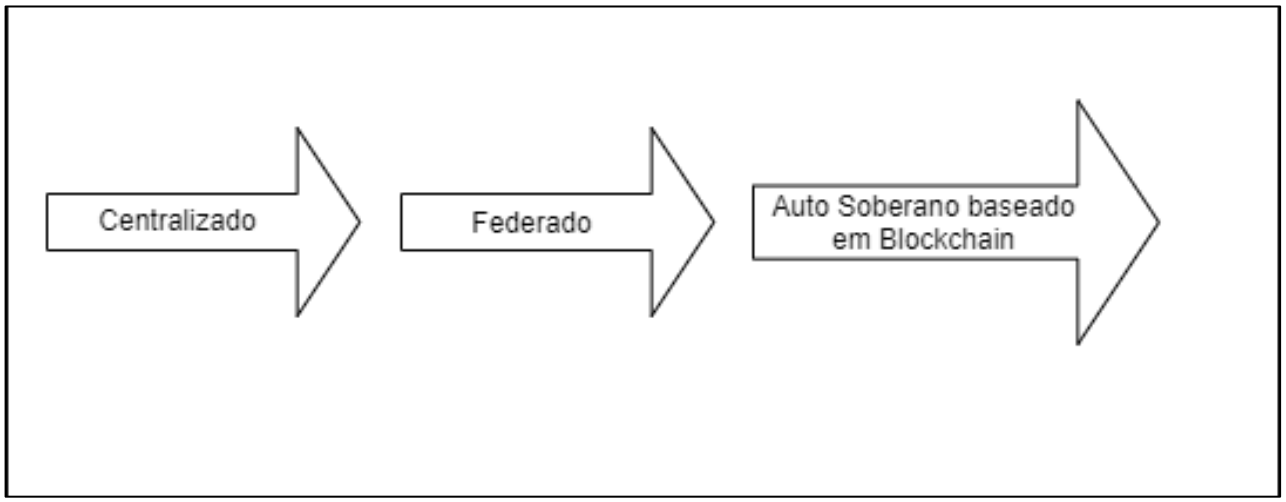

Figura 4. Evolução dos modelos de identidades digitais. Adaptado de AHMED et. al. (2020)

2.5.1 Centralizado

O modelo centralizado é o mais antigo, nele, basicamente, a organização emite credenciais para os usuários, permitindo-lhes usar serviços. A relação de confiança entre a organização e o usuário está na senha compartilhada. Na maioria dos casos, trata-se da senha de *login* associada ao nome de usuário. A identidade do usuário é armazenada e controlada pela organização como mostra na *Figura 5*. Além disso, o usuário repete este processo e requer outras credenciais para cada organização ou sistema no qual queira obter acesso.

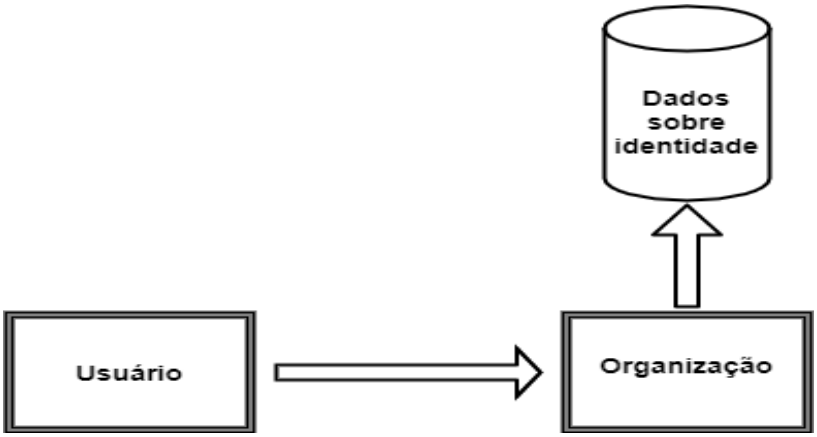

Figura 5. Modelo centralizado de *Identidade Digital*. Adaptado de NAIK et.al. (2020)

2.5.2 Federado

Uma evolução do modelo Centralizado, no entanto esse modelo procurou resolver dois problemas:

I. a carga organizacional de gerenciamento de identidade é retirada da organização, possibilitando o surgimento de um terceiro elemento, chamado *Provedor de Identidade* (IDP).

II. a responsabilidade do usuário é reduzida *vis-à-vis* a diversidade de credenciais relacionadas à identidade em uso em outros sistemas. Porém, este modelo também apresenta um problema. Trata-se da quantidade de dados pessoais e confidenciais sobre a identidade do usuário mantidos no provedor, ou seja, o usuário não tem controle sobre essas informações *Figura 6*.

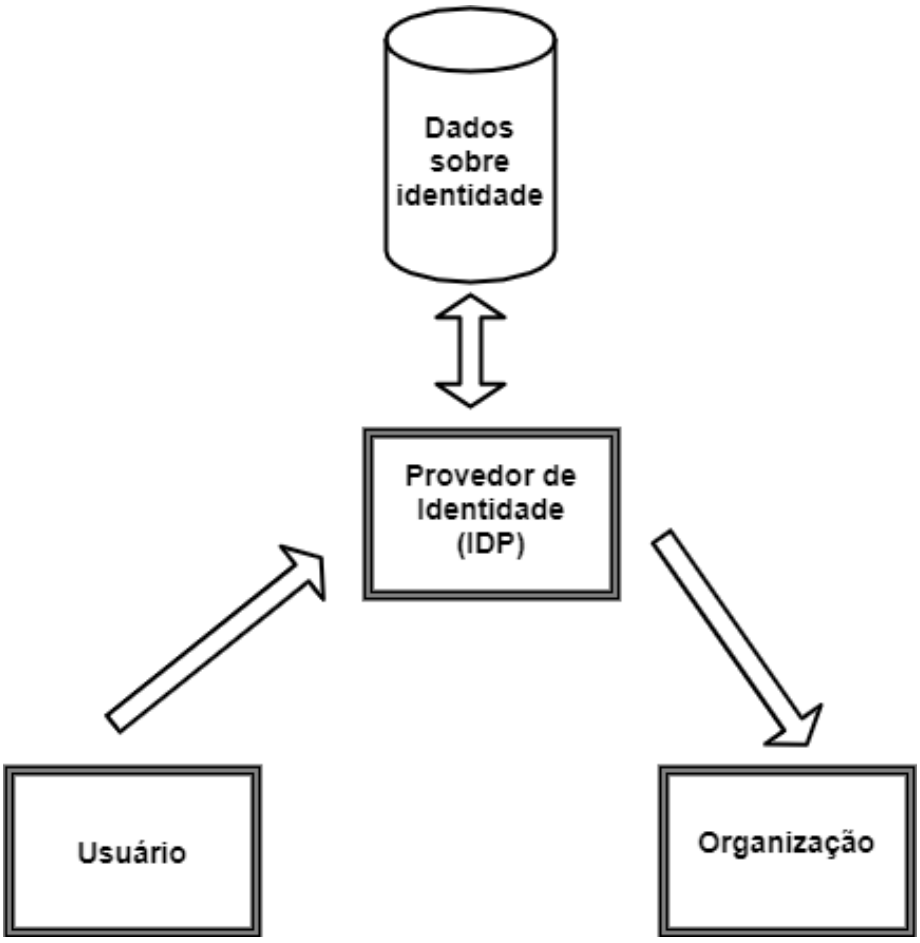

Figura 6. Modelo Federado de Identidade Digital. Adaptado de NAIK et.al. (2020)

2.5.3 Auto Soberana Baseado em Blockchain

Esse modelo foi introduzido para resolver um problema crucial em relação ao controle do

armazenamento de dados pessoais e confidenciais, cf. a *Figura 7a*, na medida que oferece ao usuário total soberania sobre a sua própria identidade. A propriedade da identidade, isto é, a posse sobre as informações privadas é mantida sobre o controle do usuário.

O modelo *Auto Soberano* é uma melhoria do modelo *Federado*, no sentido de que nessa arquitetura os provedores terceiros não tem acesso exclusivo sobre os dados dos usuários. O controle, o acesso e o direito de propriedade sobre os dados estarão de forma exclusiva sobre a responsabilidade do próprio usuário, possibilitando nessa ótica a conexão direta entre usuário e organização. Por exemplo, a *Figura 7b* mostra a situação em que uma carteira digital armazena a identidade pessoal, como também todos os dados pessoais que são controlados e mantidos pelo usuário, a partir do dispositivo escolhido por ele. Nesse contexto, o modelo *identidade digital Auto Soberana* assume três funções principais: a *função de emissor, de titular e de verificador*, dentro de um ecossistema. O emissor tem o papel de criar e emitir as credenciais para o titular. O titular, por sua vez, recebe as credenciais de emissor e compartilha quando necessário as credenciais com o verificador. Por fim, o verificador recebe e verifica as credenciais apresentadas pelo titular.

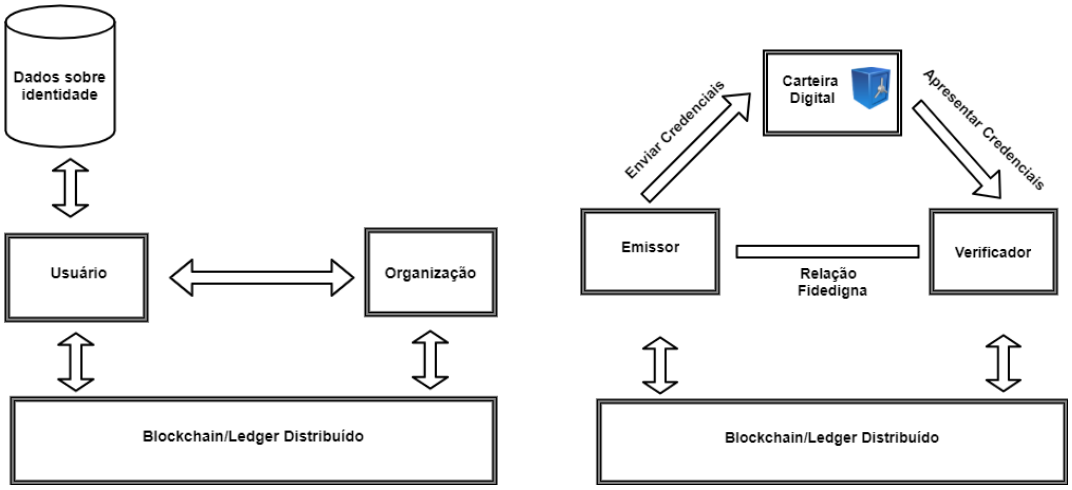

Figura 7. (a) Modelo *Auto Soberano de identidade digital*. (b) Ecossistema modelo *Auto Soberano* de *identidade digital*. Adaptado de NAIK et.al. (2020)

O modelo de *identidade digital Auto Soberana baseado em blockchain* foi adotado como base para estudo para esse trabalho e será mais detalhado em tópicos específicos.

3 Identidade Digital Auto Soberana

3.1 Introdução

Nesta seção, serão apresentados os conceitos que fundamentam o modelo de identidade *Auto Soberana* encontrados na literatura, em relação as propriedades essenciais do modelo com base em taxonomia própria. A principal motivação desta análise é entender melhor as propriedades em termos do significado semântico das propriedades e dos princípios que compõem o modelo *Auto Soberano*. Em seguida, analisa-se o impacto da identidade *Auto Soberana* com base nos princípios da *Identidade Digital*.

3.2 Conceitos iniciais

A identidade digital é um elemento central para garantir uma operação bem-sucedida em qualquer plataforma digital. No *Capítulo 2*, foram apresentados os principais modelos em relação a *identidade digital*. Em especial, conforme definição apresentada, a escolha do modelo *Auto Soberana* de *identidade digital*, nesse trabalho, é a busca da garantia necessária, para que a centralização das informações sobre e a respeito da identidade do usuário seja controlada por ele mesmo, bem como muni-lo com os métodos de controle sobre a gestão da sua própria privacidade. Nesse sentido, o usuário deve ter o poder de selecionar o que quer mostrar em relação aos seus dados pessoais e/ou confidenciais quando utiliza, por exemplo, o serviço de carteira digital.

Para DE FILIPI *et. al.* (2020), o conceito de *Auto Soberania* é uma mudança de paradigma em comparação com os demais modelos de identidades digitais. Embora, existam muitas promessas, é fato que o uso do modelo em questão ainda não encerra um consenso formado em torno da ideia. Aqui, pretende-se mostrar que a identidade de cada agente/usuário pode ser assegurada por meio dos recursos da *Auto Soberania*. Para isso, os elementos que compõe tal modelo também podem ser aplicados para garantir o uso, por exemplo, em uma arquitetura de sistema baseado em agentes de software.

Neste contexto, nota-se um crescente interesse—iniciado—no meio acadêmico em função da quantidade de publicações de artigos baseados no modelo de identidade *Auto Soberana* cf. a *Tabela 3.* Diferentes grupos de pesquisadores estão realizando experimentos

de como o modelo pode ser implantado e sustentado sobre o viés tecnológico. Por outro lado, percebe-se uma falta de coesão mútua entre tais grupos, e isso tem levado a criar noções distintas e muitas das vezes contraditórias, sobre o conceito de identidade *Auto Soberana*. A seguir são apresentadas as definições e/ou noções existentes sobre o modelo do ponto de vista da literatura especializada. Visa-se, portanto, com essas definições fundamentar um entendimento comum sobre o tema, a fim de usá-lo como fundamento também no contexto dos agentes de software.

WANG *et.al.* (2020) entende também que a noção de identidade *Auto Soberana* é um conceito recente, sem a existência de um acordo fechado em torno da terminologia. De modo geral, se destina a fortalecer o direito de *divulgação seletiva* dos diferentes aspectos da *identidade do indivíduo*, como também dos componentes que rege os diversos domínios dos dados pessoais. Esse direito deve ser aplicado, independentemente da patente do provedor ao solicitar o acesso aos dados do indivíduo, seja uma organização. De modo específico, a identidade *Auto Soberana* se refere à ideia de que os indivíduos devem manter o *controle* sobre seus dados pessoais e, até certo ponto, sobre as representações de suas identidades (ou personas) dentro do modelo que gerencia a identidade. Reforçando a ideia da capacidade de controle de quem tem o direito de acessar informações específicas sobre eles com muitas granularidades distintas.

DER *et. al.* (2017), afirma que o modelo de identidade *Auto Soberana* possibilitou para as pessoas ter maior controle sobre a presença digital. No entanto, esse controle atribui exclusivamente a pessoa, a responsabilidade pelas medidas tomadas para estabelecer e manter a privacidade e a confiabilidade. Nesse modelo, não basta apenas provar a autenticidade das informações, mas também é necessário comprovar a autenticidade das provas apresentadas.

Embora o modelo exija que os indivíduos sejam os únicos detentores das informações sobre si mesmos, uma condição importante para a validação do modelo é que a identidade do indivíduo não fique armazenada em qualquer plataforma sem o *consentimento* do usuário, nem controlada por determinado operador. No entanto, ao em vez disso, as identidades digitais permanecem portáteis e interoperáveis por várias plataformas para conferir a liberdade de escolha do operador da identidade, isto é, aquele ao qual o usuário mais confia, e assim mudar de um operador para outro, se assim o desejar.

Para TOTH *et. al.* (2019), de modo inegável, a identidade digital *Auto Soberana* promete resolver a crise de identidade. As leis sobre privacidade, geralmente requer dos provedores ações para salvaguardar e garantir que as informações privadas sejam usadas apenas para fins consentidos. Visto por outro lado, dar aos cidadãos a *soberania explícita*

sobre a própria *identidade digital* é uma promessa para aumentar a privacidade. Além disso, os prestadores de serviços de informação não precisarão coletar tantos dados privados sobre o usuário, facilitando a responsabilidade em salvaguardar dados privados. A *Auto Soberania* promete, portanto, fornecer identidades para aqueles que perderam ou foram despojados de suas próprias identidades. Essas pessoas podem adquirir identidades digitais atestadas por partes legítimas, mesmo quando não podem ser adquiridas por meio dos emissores de identidade designados.

3.3 Taxonomia, propriedades e requisitos

Os *requisitos* que compõe o modelo de identidade *Auto Soberano* foram inicialmente apresentados por ALLEN (2016), agrupados por categoria na *Figura 8*:

Controle	Portabilidade
Proteção	Existência
Interoperabilidade	Persistência
Transparência	Minimização
Consentimento	Acesso

Figura 8. Princípios de Allen para identidade *Auto Soberana*. ALLEN (2016).

Os requisitos apresentados na *Figura 8* fundamentam a ideia a respeito do que seria o modelo de identidade *Auto Soberana*, no entanto, mesmo em ALLEN (2016), as definições sobre o *consenso* e como as regras são aplicáveis ao modelo *Auto Soberano* não foram plenamente estabelecidas. Ainda em relação aos requisitos, ZYSKIND *et. al*. (2015) reforça-se a necessidade da *transparência*, da *auditoria* e do *controle* refinado sobre os dados. Já que o usuário deve saber de modo completo quais dados estão sendo coletados sobre ele e como foram acessados, podendo caso a caso revogar o acesso a dados coletados anteriormente.

No entanto, dado os conceitos e atributos encontrados em FERDOUS *et. al.* (2019), TOTH *et. al.* (2019), ALLEN (2016), ANDRIEU (2016) e TOBIN *et. al.* (2017), entendeu-se que necessário organizar uma *taxonomia* das características encontradas para apresentar de forma ampla os *conceitos fundamentais* que compõe o modelo *Auto Soberano*, cf. a *Figura 9*. É importante enfatizar que as propostas apresentadas pelos autores visam validar apenas as propriedades necessárias na criação de uma aplicação baseada em identidade digital *Auto Soberana*, em que o objetivo é assegurar o *controle da identidade pelo agente* como *fonte*

confiável. Os modelos buscam mostrar, de forma inovadora, o controle realizado pelo agente/usuário sobre as próprias informações pessoais, habilitando um compartilhamento proativo dos dados dos locais quando esse agente atua em rede.

Figura 9. Taxonomia para modelo de identidade *Auto Soberana*.

Com base na *Figura 9*, as próximas seções detalham cada uma das características presentes na taxonomia, com o objetivo de apresentar a respectiva fundamentação,

nomenclatura e respectivos trabalhos que originaram ou agruparam tais conceitos.

3.3.1 Fundamentos

As propriedades fundamentais para embasar o modelo de *Auto Soberania* foram agrupadas em ALLEN (2016). Tais agrupamentos representam as principais propriedades sem as quais o modelo de identidade digital não existiria. As propriedades são retratadas como segue:

I. *Existência*. Uma identidade *Auto Soberana* deve permitir o usuário codificar digitalmente as suas próprias características para afirmar a sua existência no domínio digital. Este é, essencialmente, uma quase-representação de si mesmo no formato digital. O objetivo é tornar pública e acessível os aspectos delimitados da identidade do indivíduo. Uma observação a ser feita sobre a propriedade da *Existência* é que um agente malicioso não deve ter ao seu dispor de mecanismos para criar uma nova identidade somente para obter benefício próprio, para isso não ocorrer torna-se necessário garantir que as propriedades de Segurança sejam verificadas de modo integral.

II. *Autonomia*. Uma identidade *Auto Soberana* deve apoiar totalmente a autonomia na gestão e na administração das informações.

III. *Posse*. O usuário deve ser o proprietário final de uma identidade *Auto Soberana*. Isso se aplica a qualquer informação codificada da identidade.

IV. *Acesso*. O usuário deve ter acesso irrestrito à sua própria identidade em formação. Ele deve ser capaz de recuperar cada informação. Não deve existir dados ocultos e nenhuma barreira. Isso não significa que um usuário pode modificar todas as declarações associadas sobre si, mas significa que ele deve estar ciente delas. Também não significa que os usuários tenham acesso aos dados de outras pessoas; eles tem acesso apenas aos seus próprios.

V. *Fonte única*. Um usuário deve ser a única fonte de verdade sobre sua própria identidade. Ele deve ser o guardião máximo para identidade e distribuí-la quando necessária. Isso garante que a terceira parte não pode conspirar para trocar os dados da identidade sem conhecimento do usuário.

Para facilidade de uso, no entanto, o usuário pode delegar esta tarefa a um agente autônomo/software que está sob seu controle.

3.3.2 Segurança

Neste grupo são apresentadas as propriedades que são usadas para garantir a segurança da identidade *Auto Soberana*. Essas propriedades são cruciais para assegurar que o conceito de segurança está fortemente acoplado ao modelo da identidade *Auto Soberana*. Essas propriedades foram descritas e agrupadas em TOBIN (2017):

I. *Proteção*. Uma identidade *Auto Soberana* deve estar bem protegida com os mais recentes métodos criptográficos que satisfazem a *confidencialidade, integridade e autenticidade* (CIA) e propriedades de *não-repúdio*. Cada interação envolvendo uma identidade deve ser autorizada e a correspondente entidade devem ser devidamente autenticadas. Para qualquer identidade, as informações devem ser armazenadas de forma segura e transmitida por meio de um canal seguro. Em qualquer sistema para manusear tal identidade deve suportar um método de controle de acesso refinado para garantir o nível necessário de controle do usuário sobre sua identidade.

II. *Disponibilidade*. Uma identidade *Auto Soberana* deve estar prontamente disponível e acessível em diferentes plataformas quando exigido por seu proprietário. Deve ser robusta e suficiente para ser recuperável mesmo com a perda de um armazenamento específico onde esses dados estão armazenados.

III. *Persistência*. Uma identidade *Auto Soberana* deve ser persistente, pelo menos enquanto for exigido por seu proprietário. Para reclamações de terceiros, ela deve ser persistente até a autoridade declarada deixar de existir. As identidades devem ser de longa duração e atualizáveis, e o proprietário deve ser capaz de esquecê-las quando não mais necessário.

3.3.3 Controle

Nesse grupo, coloca-se as propriedades que podem ser usadas para controlar quaisquer dados de identidade. As propriedades pertencentes a este grupo são descritas em ANDRIEU (2016):

I. *Capacidade de escolha*. Um usuário deve ter o controle final para decidir quando desejado liberar os dados da identidade para quaisquer entidades em um contexto específico.

II. *Divulgação*. Quando os dados de uma identidade são liberados para uma terceira parte, o usuário deve ter a capacidade de divulgar seletivamente os atributos específicos, isso é necessário para assegurar ao usuário o direito de exercer o controle sobre seus dados.

III. *Consentimento*. Cada parte dos dados de identidade deve ser liberado para uma terceira parte somente após o correspondente consentimento do usuário em fazê-lo.

3.3.4 Flexibilidade

A fim de garantir que uma identidade *Auto Soberana* possa operar em diferentes sistemas, o modelo precisa ser tão flexível quanto possível. Nesta categoria é apresentada as propriedades relacionadas com a flexibilidade. As propriedades desta categoria foram encontradas em ALLEN (2016) e TOBIN *et. Al.* (2017):

I. *Portabilidade*. Uma identidade deve ser portátil, o que deve garantir que a identidade parcial de um usuário possa ser transferida para um meio ou plataforma quando o anterior meio ou plataforma desaparecer. Por outro lado, uma identidade para ser portátil precisa garantir a persistência das informações por um longo período de tempo.
II. *Interoperabilidade*. Em função da natureza heterogênea da Internet e dos serviços *online*, uma identidade *Auto Soberana* deve ser projetada de tal forma que possa atingir o nível máximo de interoperabilidade. Deve assegurar compatibilidade com versões anteriores de sistemas de identidade legados por um período de tempo para garantir uma interação entre sistemas.
III. *Minimização*. A divulgação da identidade deve ser minimizada tanto quanto possível. A identidade deve ser flexível o suficiente para garantir que um usuário possa atingir seus objetivos desejados com o fornecimento mínimo dados sobre a identidade para realizar a tarefa em mãos.

3.3.5 Sustentabilidade

As propriedades para garantir a sustentabilidade de identidade *Auto Soberana* está listada nesta categoria, encontras e agrupadas em ANDRIEU (2016) e TOBIN *et. al.* (2017):

I. *Transparência*. O sistema que gerência a identidade *Auto Soberana* deve ser transparente o suficiente para todos os envolvidos entidade. O usuário deve estar ciente de todas os tipos de identidades existentes e as correspondentes interações ocorridas. O sistema e o algoritmo devem permitir uma fácil recuperação de tal interação para garantir a transparência. Outra maneira de conseguir isso é garantir que o sistema seja totalmente código aberto, com a intenção de permitir a qualquer pessoa examinar os recursos internos e os algoritmos.

II. *Padrão*. O modelo de deve ser baseado em padrões abertos para garantir a máxima portabilidade, interoperabilidade, a adoção e a sustentabilidade.

III. *Custo*. O custo para criar, gerenciar e adotar um modelo de identidade *Auto Soberana* deve ser o mínimo possível. Caso contrário, criará obstáculos desnecessários para a adoção em larga escala.

Como visto na *Figura 9,* a taxonomia do modelo informa os *requisitos necessários* que fundamentam o modelo de identidade *Auto Soberano*, objetivando reforçar a *visão* de que o *indivíduo está no controle dos próprios dados* relacionados à própria identidade. Nesse sentido, pode ser entendido como verdadeiro os movimentos em função da qualidade e dos valores propagados por meio do formato *descentralizado de identidade*. No entanto, não se deve confundir os requisitos apresentados como dogmas. Nesse caso, não se deve se abster de questionar e continuar a refiná-los quando necessário.

3.4 Princípios aplicados

Para assegurar a identidade digital dentro do modelo *Auto Soberano* para um agente/usuário, CAMERON (2005) propôs *princípios* de como a identidade de um usuário deve ser tratada e liberada. Os princípios são brevemente apresentados a seguir.

I. *Controle e consentimento do usuário*: a aplicação do modelo deve apenas revelar informações que identificam um usuário de acordo com o consentimento dele.

II. *Divulgação mínima com uso restrito*: deve-se garantir a menor divulgação de informações sobre a identificação e ainda obter os melhores resultados de uso. Apresentar credenciais de identificação completa pode revelar mais informações do que o necessário. A capacidade de limitar as informações apresentadas a partir de uma credencial é importante para manter a privacidade por meio do princípio de divulgação mínima.

III. *Interação entre as partes envolvidas*: os métodos de identidade digital devem ser projetados de forma que a divulgação de informações de identificação seja limitada às partes, garantindo o espaço necessário e justificável em um determinado relacionamento.

IV. *Identidade Dirigida*: deve ser oferecido suporte a identificadores do tipo multidirecional para uso por entidades públicas e identificadores unidirecionais para uso por entidades privadas. A ideia é facilitar a identificação correta do agente

operador evitando a liberação desnecessária de identificadores. Por exemplo, o emissor da credencial, o *Empregador* de *Alice*, tem um identificador público. Um identificador público é necessário para emitir credenciais, uma vez que o verificador desejará consultar o emissor como parte da verificação da credencial. O *Banco* que *Alice* é cliente provavelmente também tem um identificador público, mas não desempenha nenhum papel nessa troca de credenciais. *Alice* trocou identificadores privados com seu *Empregador* e com o *Banco*. Esses identificadores privados formam a base do relacionamento criptográfico que *Alice* mantém com essas instituições. Os identificadores que o *Empregador* e o *Banco* dão a *Alice* também são privados, destinados apenas ao relacionamento com *Alice*, o exemplo da aplicação está representado na *Figura 10*.

V. *Interoperabilidade entre tecnologias*: a aplicação deve canalizar e permitir diferentes tecnologias de identidades digitais, a razão para isso é que não deve haver uma aplicação centralizada do tipo monolítica, mas permitir a diferenciação deste para que as aplicações possam comunicar por meio de protocolos (a exemplo uma aplicação comunica com outra por meio da entrada de dados por meio de uma API).

VI. *Integração humana*: o usuário do tipo ser humano é um componente do sistema distribuído integrado por meio de recursos de comunicação *homem-máquina* que oferecem proteção contra-ataques de identidade.

VII. *Experiência do usuário em todos os contextos*: deve-se garantir aos usuários uma experiência simples e consistente, permitindo a separação de contextos por meio de vários operadores e tecnologias.

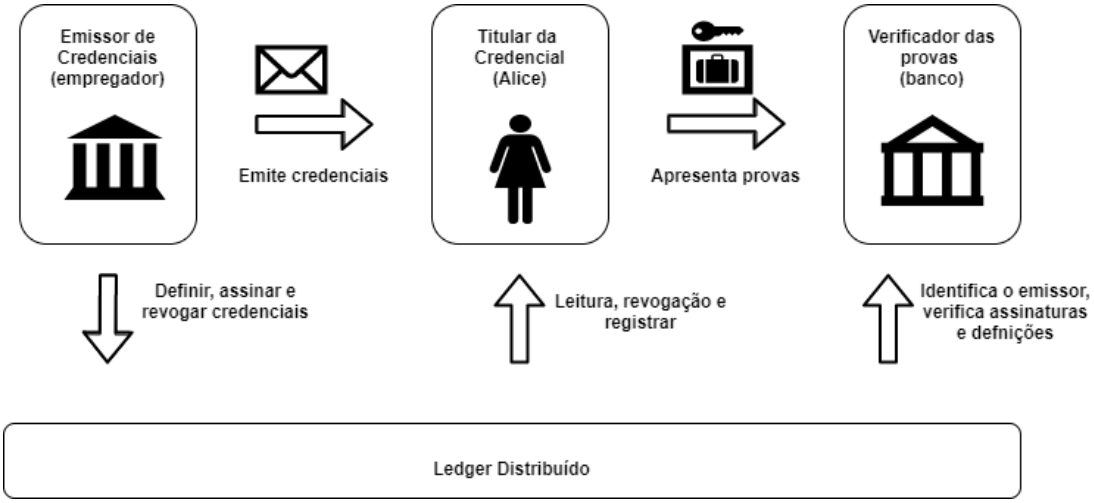

Figura 10. Representação do princípio da *Identidade Dirigida*. Cameron (2005).

3.5 Arquitetura

Em estudos recentes, soluções envolvendo o modelo *Auto Soberano* de identidade integrados em conjunto com aplicações baseadas em *Ledger distribuídos* tem surgido como forma de projetar propostas de identidades digitais descentralizadas, aplicadas em diferentes cenários. A seguir, apresentamos na *Tabela 3* os respectivos referenciais que têm como objetivo comparar soluções a partir da verificação da existência arquitetura ou de componentes baseados no modelo *Auto Soberano*. Em DIB *et. al*. (2020) e LIU *et. al.* (2020) buscou-se estabelecer a relação entre o *conceito* de identidade digital e de modelo *Auto Soberana* em conjunto com os respectivos *componentes* de *arquitetura* dentro do contexto de *Ledger distribuído*.

Tabela 3. Referencias teóricos aplicados ao modelo *Auto Soberano* de *identidade digital*. A presença da característica (✓) ou a ausência (●). □

Trabalho	Conceito de Identidade Digital	Identidade Digital Soberana	Componentes de identidade	Arquitetura
BANDARA *et. al*. (2021)	✓	✓	✓	✓
ABID *et. al*. (2021)	✓	✓	✓	✓
XIAO *et. al*. (2021)	✓	✓	✓	✓
NAIK *et. al*. (2020) a	✓	✓	✓	✓
NAIK *et. al*. (2020)b	✓	✓	✓	✓
ABRAHAM, *et. al*. (2020)	✓	✓	✓	✓
AHMED *et. al*. (2020)	✓	✓	✓	✓
GEBRESILASSIE *et. al*. (2020)	✓	✓	✓	✓
GILANI *et. al*. (2020)	✓	✓	✓	✓
HOUTAN *et. al*. (2020)	✓	✓	✓	✓
LIU *et. al*. (2020)	✓	✓	✓	●
INOUE *et. al*. (2020)	✓	✓	●	✓
HASAN *et. al*. 2020)	✓	✓	✓	✓
LUX *et. al*. (2020)	✓	✓	✓	✓
SOLTANI *et. al*. (2020)	✓	✓	✓	●
MUKTA *et. al*. (2020)	✓	✓	✓	✓
STOKKINK *et. al*. (2019)	✓	✓	●	✓
LESAVRE *et. al.* (2019)	✓	✓	✓	✓
BOKKEM *et. al*. (2019)	✓	✓	●	●
REN *et. al.* (2019)	✓	✓	✓	✓
TOTH *et. al.* (2019)	✓	✓	✓	✓
MELL *et. al*. (2019)	✓	✓	●	✓
HADDOUTI *et. al.* (2019)	✓	✓	✓	✓
FERDOUS *et. al.* (2019)	✓	✓	✓	●
KASSEM *et. al.* (2019)	✓	✓	●	●
MUHLE *et. al.* (2018)	✓	✓	✓	✓
DER *et. al.*. (2017)	✓	✓	●	●
BAARS *et. al*. 2016	✓	✓	✓	✓

Em contraste com a maioria dos sistemas de gerenciamento de identidade, em que o provedor de serviços fica no centro da identidade, no modelo de identidade *Auto Soberana* o

elemento central é o *usuário*. Para MUHLE *et. al*. (2018), GILANI *et. al*. (2020) e DIB *et. al*. (2020) a *arquitetura* que compõe o modelo *Auto Soberano* pode ser vista na *Figura 11*, com a representação dos diferentes atores que compõe tal modelo.

Nessa arquitetura, inicialmente na requisição o *emissor* emite-se (pelo menos parte de) a identidade, atestando os atributos do usuário. Por outro lado, qualquer parte confiável que necessite identificar o usuário verá as partes da identidade do usuário que seja relevante para aquela situação. Em seguida, para atestar a identidade a *parte confiável* precisa ter um relacionamento de confiança com o *emissor* da requisição. Além disso, é preciso enfatiza a existência de uma camada importante acrescentada no modelo *Auto Soberano* que é uso da *arquitetura distribuída*, em especial com uso da tecnologia *blockchain*, o qual é apresentada em tópicos posteriores.

Para STOKKINK *et. al*. (2018), a *proteção da informação* é uma propriedade importante na arquitetura do modelo da identidade *Auto Soberana*. Nessa propriedade, como o usuário tem o controle sobre a própria privacidade e em conjunto o direito de ser esquecido, há a necessidade de divulgar informações em partes e sob demanda. Além disso, uma vez compartilhada, a informação que a outra parte recebe pode não ser útil para a reutilização. Em outras palavras, as informações recebidas devem ser verdadeiras apenas para a parte à qual a informação foi divulgada.

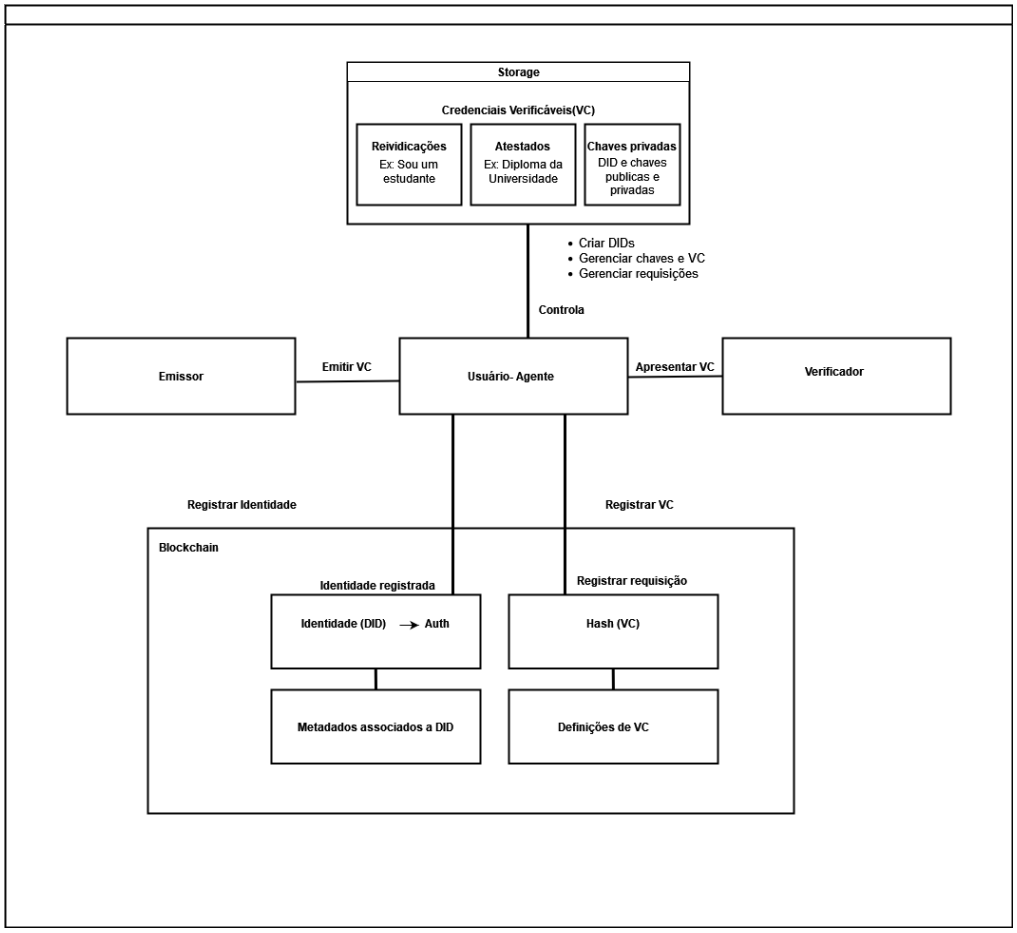

Figura 11. Arquitetura da identidade *Auto Soberana*. Adaptada de MUHLE (2018), GILANI (2020) e DIB (2020).

Para DIB *et al*. (2020), no modelo descentralizado de identidade digital não há a dependência de um ou de um conjunto de provedores de serviços para estabelecer e/ou gerenciar identidades, ao invés disso, existe apenas a dependência de um armazenamento de dados privado (*storage*) (cf. *Figura 11*), com a função de manter os atributos da identidade e de um dispositivo digital para gerenciar o ciclo de vida da identidade. O armazenamento de dados pode assumir, por exemplo, a forma de um telefone celular, computador pessoal ou armazenamento em nuvem privada. No entanto, deve-se manter os *atestados de confiança*, das *relações realizadas* por meio dos serviços com governos, bancos ou empregadores. A entidade escolhe o dispositivo digital e qual atestado ou quais dados dos atributos vai compartilhar no contexto ou no propósito que o compartilhamento está ocorrendo. Ao fazer isso, a entidade mantém o controle sobre seus atributos de identidade e os respectivos atestados associados.

Sobre a implementação:

Existem diferentes maneiras de implementar o modelo de identidade *Auto Soberano*, no entanto, em todas as abordagens há a necessidade de se resolver problemas semelhantes. Em

sua maioria está na forma de garantir a confiança nas informações sem recorrer a alguma autoridade central. Para se ter uma ideia de como isso pode funcionar, os seguintes componentes devem ser considerados.

I. Identificador Único Descentralizado (DID):

O modelo de identidade digital *Auto Soberano* é presentado por meio de uma identidade descentralizada, a qual contém um identificador único. Para ALZAHRANI (2020) esse *identificador descentralizado* (DID) trata-se do método de autenticação autogerenciável cujo padrão foi estabelecido foi pela World Wide Web Consortium (W3C). Os DIDs atuam em conjunto com *credenciais verificáveis* (VCs), com objetivo de estabelecer a padronização contínua em relação a preservar a privacidade. Ambas as abordagens assumem que os registros estejam descentralizados e imutáveis. No entanto, nos padrões estabelecidos pelo W3C, a forma como o registro é implementado foi deixado em aberto. Em relação a estrutura, o identificador constitui-se em uma chave pública e outra chave privada. A primeira pode ser compartilhada publicamente com outras entidades, enquanto a outra deve ser mantida em segredo pelo titular, já que ao utilizar a chave privada, a entidade pode provar digitalmente a propriedade do DID.

II. Documentos DID

Em ALZAHRANI (2020) e W3C (2019), um *DID* está associado a um documento cuja estrutura segue o representado na Figura 12. O objetivo deste documento é descrever a estrutura das chaves, com os protocolos necessários para a autenticação e os devidos pontos de entradas dos serviços que irão interagir com a entidade identificada. Especificamente, um documento *DID*, conforme definido pelo W3C, inclui seis componentes: o próprio *DID*; materiais criptográficos, como *chaves públicas* usadas para autenticação; *protocolos criptográficos* para interagir com o sujeito *DID*; a lista de *endpoints*; *auditoria de carimbos de data/hora* e uma *assinatura JSON-LD* para verificar a integridade do documento.

```
{
  "id": "did:example:1234",
  "publicKey": [{
    "id": "did:example:1234#key1",
    "type": "Ed25519VerificationKey2018",
    "publicKeyBase58" : "..."
  }
  ],
  "authentication": [
    "did:example:1234#key1",
  ],
  "proof":{
    "type": "LinkedDataSignature2015",
    "created": "2020−02−08T16:02:20Z",
    "creator": "did:example:1234#key1",
    "signatureValue": ".."
  }
}
```

Figura 12. Estrutura de um documento DID. ALZAHRANI (2020)

III. Ledger Distribuído

Para SUNYAEV (2020), uma forma de tornar os DIDs descentralizados é implementá-lo sobre um *Ledger Distribuído*. A finalidade é fornecer a infraestrutura pronta para que ocorra o gerenciamento os dados de forma descentralizada e confiável. Além disso, espera-se que as credenciais das entidades sejam autenticadas com os carimbos de data/hora de modo eletrônico. O que se pretende é assegurar uma prova de quando a credencial foi criada, bem como também garantir que não houve qualquer adulteração da credencial.

IV. Credenciais verificáveis

A ação de criar DIDs com os respectivos documentos associados e ainda registrá-los de forma distribuída podem não ser suficientes para habilitar todos os recursos de uma infraestrutura de identidade descentralizada. De forma complementar, há a necessidade de construir outro bloco denominado de *Credenciais Verificáveis* (VCs).

Em LUX *et. al*. (2020) uma *VC* é uma informação criptograficamente confiável sobre o histórico de uma entidade, geralmente é compartilhada como uma prova confiável fortemente vinculada a um DID público. Normalmente, essa prova confiável tem a forma de uma assinatura digital e pode ser verificada usando a chave pública do *DID do emissor*. Como exemplo, uma *Credencial Verificável* pode ser representada por meio de um certificado emitido digitalmente.

Na estrutura de identidade descentralizada da *Figura 12*, as *VCs* devem ser

transferidas de forma que sejam compreensíveis e utilizáveis por qualquer outro sistema. Se isso não ocorrer, as credenciais devem ser analisadas manualmente, em consequência podem impedir a automatização do fluxo de informações. Para lidar com esse problema, esforços têm sido criados para que ocorra a padronização das estruturas e do conteúdo de uma VC. Para W3C o formato mais aceito está na estrutura *JSON*.

V. Armazenamento

Para permitir o uso das *credenciais* e das chaves privadas associadas aos *DIDs* há a necessidade de que essas estejam armazenadas em algum lugar para disponibilizá-las quando necessário. Armazenar essas informações é crucial para qualquer sistema de identidade descentralizado. Uma forma de armazenar esses dados está no uso dos dispositivos pessoais, como *smartphone, laptops* ou outras soluções seguras fornecidas por terceiros. Em DIB *et. al.* (2020), esse controle sobre armazenamento dos dados da própria entidade relaciona-se fortemente com o conceito para o modelo *Auto Soberano* da identidade digital. Por outro lado, ter os dados sob o controle do usuário-agente permite maior interoperabilidade, para permitir o emprego desses dados em várias plataformas para diferentes fins, resguardando a identidade do usuário de ficar presa em uma plataforma.

VI. Carteiras digitais privadas

Para DIB *et. al.* (2020), para implementar o modelo de identidade digital descentralizada é preciso utilizar ferramentas para gerenciar os DIDs, chaves privadas e as credenciais verificáveis. Essas ferramentas são atualmente chamadas de “carteiras” digitais. Essas carteiras podem vir na forma de aplicativos para celulares, *software* ou na forma *hardware* próprio. Mantendo todos os aspectos da identidade descentralizada, o elemento essencial da carteira digital é permitir que o controle fique de modo exclusivo com o usuário.

3.6 Fluxo de trabalho

O fluxo de trabalho que compõe o modelo de identidade *Auto Soberana* pode ser visto cf. a *Figura 13*. Inicialmente, ocorre a solicitação de conexão entre o usuário e o provedor de serviços. A interação inicia pelo usuário, pois é ele que tem o controle e a posse em relação a identidade digital *Auto Soberana*. No fluxo de interação, o provedor de serviços é representado por meio de um serviço *online*, aplicativo ou qualquer outro meio de comunicação que represente esse serviço. Nessa interação é enviado um *DID* para comunicar com o usuário para que a identidade do provedor de serviços possa ser verificada.

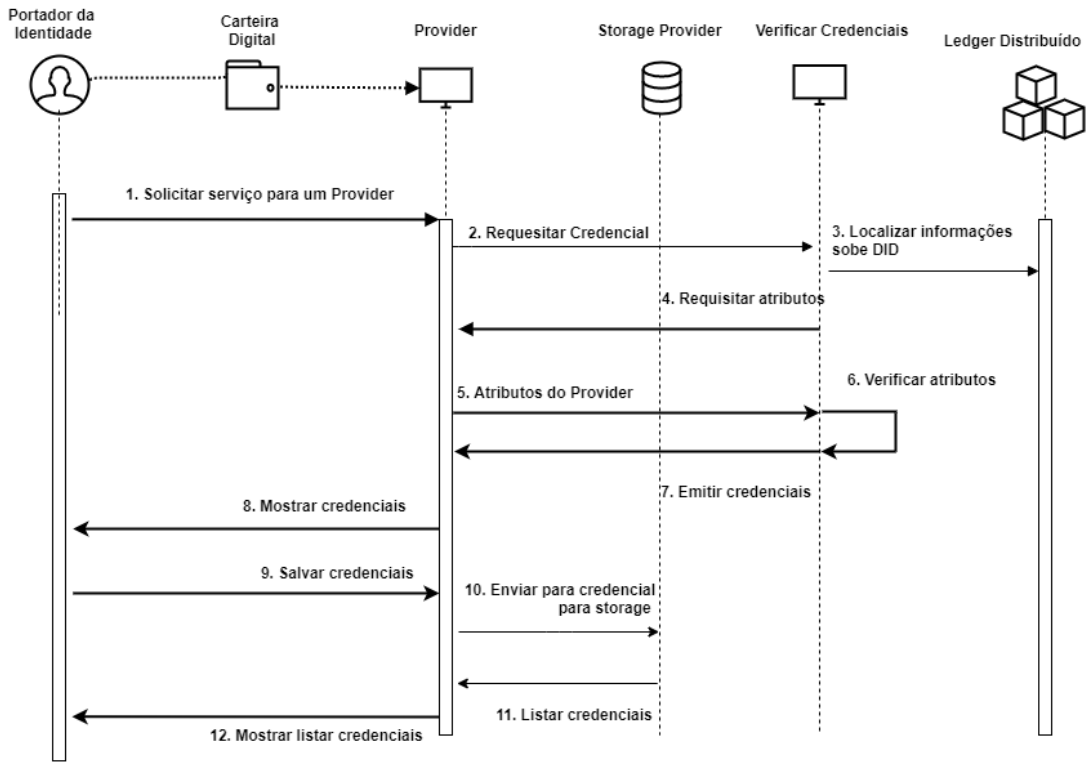

Figura 13. Fluxo de trabalho do modelo da identidade digital *Auto Soberana*. Adaptada de DIB (2020) e LUX (2020)

O provedor de serviços também deve receber o *DID* do usuário para que ele possa verificar e assegurar a comunicação com o verdadeiro dono da identidade. Certamente, para que a comunicação e verificação sejam feitas, os dados relacionados tanto do provedor de serviços quanto do usuário são recuperados das informações disponibilizada no *Ledger*. Uma vez estabelecido o canal de comunicação seguro entre o usuário e o provedor de serviços, quaisquer as credenciais de ambos os agentes podem ser enviadas, recebidas e verificadas.

A *Figura 14*, exemplifica o recurso de identidade *Auto Soberana* utilizado em conjunto com o processo de autenticação realizada pelo usuário a partir do uso de um dispositivo de *celular*. Em TOTH *et. al.* (2019), os recursos utilizados na identidade não revelam a autenticação dos dados fora do contexto. Além disso, o método de identidade é separado do modo lógico de autenticação do dispositivo. Porém, a autenticação pode ser controlada pela identidade do proprietário, criando um vínculo forte a partir das identidades digitais do proprietário. A arquitetura valida a propriedade essencial do controle e do acesso sobre as identidades digitais. Os proprietários são, portanto, capazes de controlar quais informações privadas podem ser divulgadas.

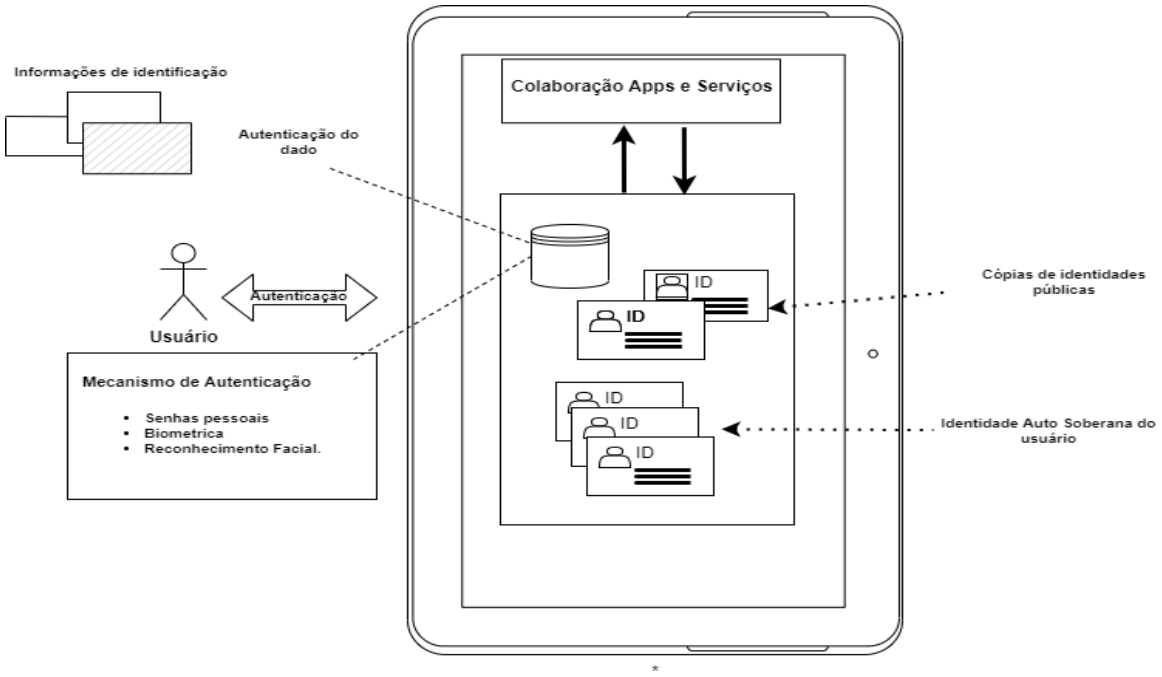

Figura 14. Modelo de Identidade Auto Soberana: o dispositivo com uma identidade instalada encapsula dados de autenticação—o proprietário pode selecionar um serviço para interagir de forma segura com outras partes. Adaptado de TOTH *et. al.* (2019).

Explicado o funcionamento do modelo de identidade *Auto Soberana*, uma outra questão a ser abordada, está em como garantir autenticidade ao modelo, ou quais são os métodos válidos que comprovam a fidedignidade. Em LIU *et. al.* (2020) e FERDOUS *et. al.* (2019) para resolver essa questão, eles apresentaram a ideia de que os componentes da identidade digital seguem um ciclo de vida de componentes, sendo a autenticidade parte de desse ciclo. No entanto, para TOTH *et. al.* (2019) a garantia da autenticidade pode-se dar por meio *de provas*, de *atestados* e de *selos digitais*. Por exemplo, se a abordagem estivesse no modelo centralizado de identidade digital, a *comprovação* e o *atestado de veracidade da identidade* estariam no fornecimento de garantias que caracterizam o proprietário, revelando ou não se é o verdadeiro dono da informação ou algum impostor. A arquitetura se assemelharia ao das identidades físicas, a exemplo da carteira de motorista e dos passaportes.

Com base no modelo apresentado na *Figura 15A*, o *emissor* registra a identidade digital do solicitante, que por sua vez será comprovada e atestada. O *solicitante* usa o método de identidade para fornecer informações de identificação pessoal para *provedor* ou para o *emissor* da identidade. O *emissor* detém a base de identidades e o conjunto de dados fornecidos para comprovar as reivindicações da identidade digital do *solicitante*.

Em seguida na *Figura 15B*, quando os proprietários utilizam a identidade digital para

realizar transações de forma síncrona ou assíncrona, as partes confiáveis podem usar o registro de identidade para verificar a existência das identidades digitais apresentadas. Se a transação for verificada com sucesso, o *emissor* especifica a forma de atestar a transação entre agente usuário e provedor. Em seguida, envia a chave privada para criar o *selo digital*, para vincular o atestado e a identidade digital do *emissor* junto com a identidade digital do *solicitante*. O método é semelhante a tradicional de assinatura digital.

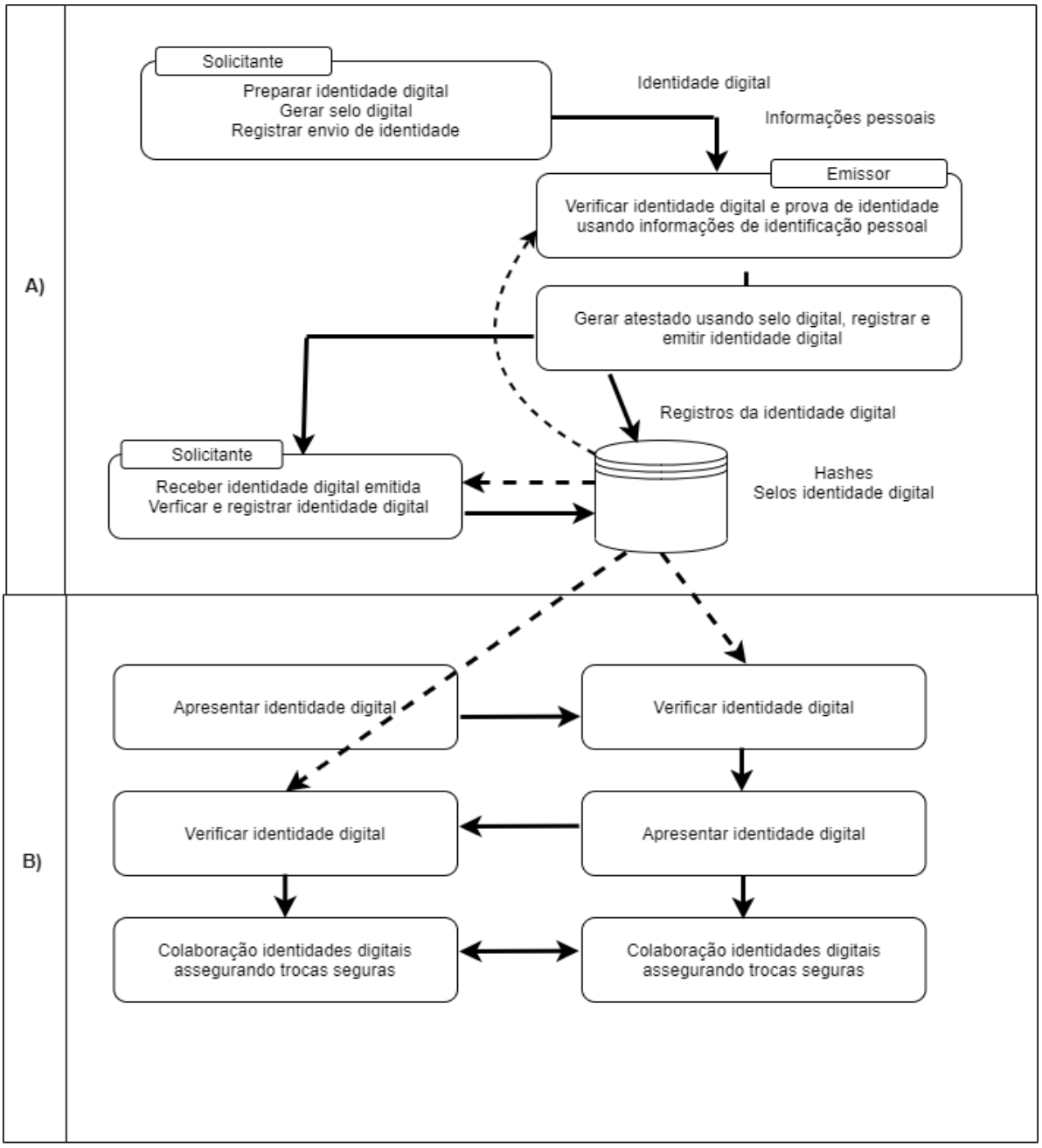

Figura 15. O proprietário solicita o registro da identidade digital perante o *emissor*. Adaptado de TOTH et. al. 2019.

De modo contrário, na *Figura 16*, dentro de uma transação entre usuários, cada um

deles pode utilizar o método de identidade digital *Auto Soberana* juntamente com o uso de *atestados* e de *selos digitais* que estão afixados nas identidades digitais para serem utilizados quando for preciso. A *parte confiável* recebe uma cópia pública da própria identidade digital, e a utiliza para verificar se o outro usuário possui e tem a custódia da identidade digital, em seguida verifica os *atestados* e *selos dos emissores*.

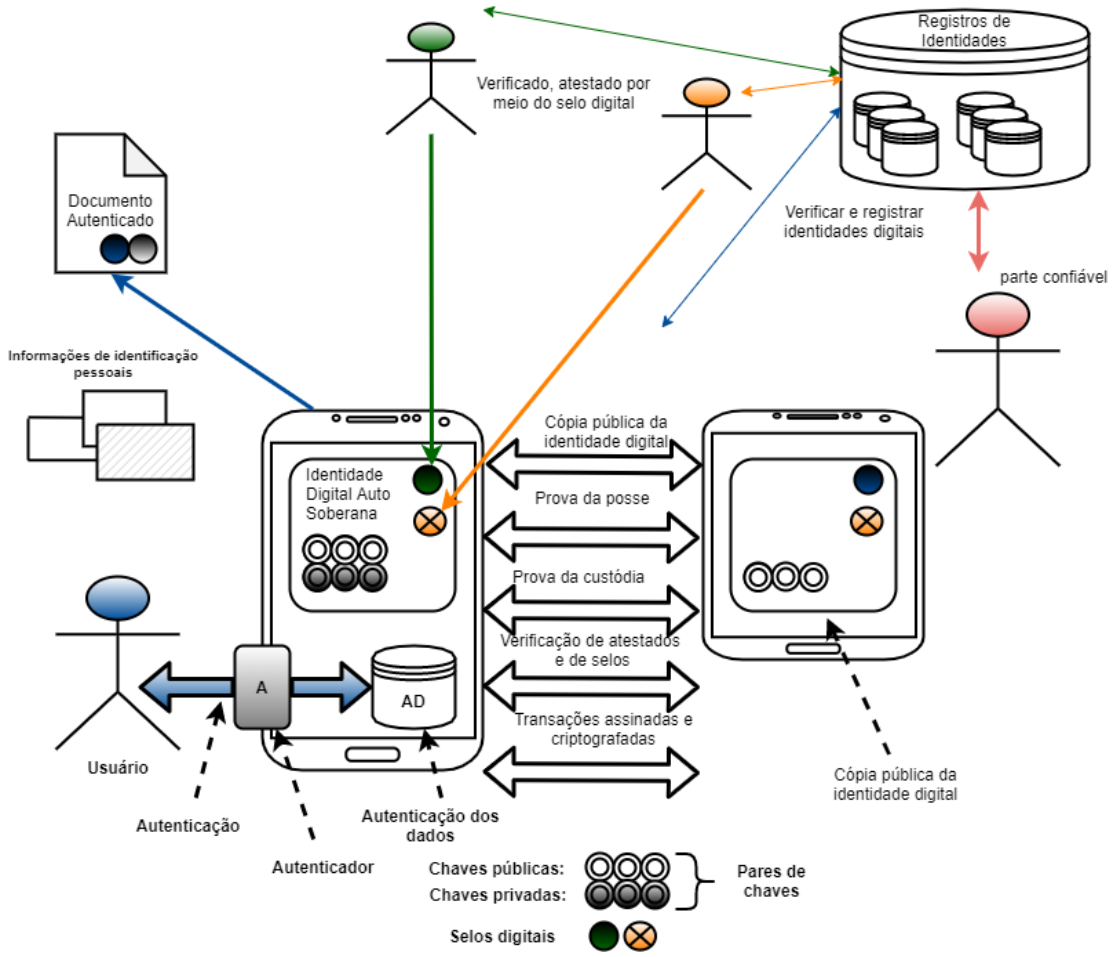

Figura 16. A identidade digital autenticada por dois emissores. Adaptado de TOTH *et. al*. (2019).

Nesse cenário, não há restrição de uso, já que a mesma identidade digital também pode ser atestada e emitida por várias partes. Os proprietários das informações podem se encontrar pessoalmente com outros usuários para emitir *selos digitais* e *atestados* em conexões diretas, por meio, por exemplo de aplicações do tipo *NFC, Bluetooth* ou *Wi-fi*. A arquitetura da identidade digital *Auto Soberana* fortalece as garantias das identidades, com a finalidade de favorecer o uso confiável das identidades digitais, com a finalidade de possibilitar o usuário provar quem de fato é.

Em TOTH *et. al.* (2019) as transações envolvendo as identidades digitais devem ser

realizadas com segurança visando evitar fraudes de falsificação de identidade. Já que as partes envolvidas, de modo pessoal, podem simplesmente compartilhar as informações e transferir dados baseados em *QR code*, ou pelo uso de USB e cartões de memória. Outra forma de compartilhamento de identidade é a troca com uso de serviços de mensagens. O registro de identidade pode ser usado para confirmar se o registro é verdadeiro e não foi corrompido. Os históricos coletados das transações ajudam os usuários comprovar a autenticidade da transação.

O método para atestar veracidade da transação com uso de *selos digitais* pode ser verificado pelas partes, apenas utilizando os pares de chaves digitais. Da mesma forma, os documentos também podem ser autenticados por meio do uso das chaves digitais para dar veracidade dos documentos. Essa abordagem mostra que é viável implantar identidades digitais, promovendo transações seguras dentro do modelo de *Auto Soberania*. No entanto, ainda que o processo para averiguar as identidades digitais seja eficiente, ainda é preciso ter métodos fortes que garantam a imutabilidade dos dados, com a finalidade de assegurar que não haja alteração dos dados durante o percurso.

Entretanto, para GULATI *et. al.* (2019), é importante estabelecer que os recursos de identidades digitais são dinâmicos e integrados por natureza. A principal vantagem é que por ser dinâmico os esforços envolvidos na verificação de uma identidade são reduzidos quando aplicados em várias plataformas. Ao incorporar a integração, dados diferentes podem ser combinados em formato de blocos com a finalidade de que a verificação possa ser feita de forma eficiente. Pode-se dizer que as várias versões da mesma identidade digital estão conectadas entre si, tornando muito mais rápida a verificação. Diferentes versões de uma identidade são criptograficamente vinculadas por meio de um código *hash*, o qual resulta numa cadeia de blocos, a semelhança das cadeias de blocos originadas do conceito de *blockchain*.

4 Identidade Digital Auto Soberana aplicada no *Blockchain*

4.1 Introdução

O conceito de blockchain (BC) surge como um *paradigma* voltado a construção de aplicações que atuam de forma descentralizada, tendo como fundamento as tecnologias de *Ledger distribuídos (DLT)* em conjunto com uma *infraestrutura computacional*. KANNENGIESSER *et. al.* (2019) reforça o uso da tecnologia de Ledger distribuído (DLT) para operações entre base de dados mantidas por dispositivos de armazenamento e de computação distribuídos fisicamente em estruturas de dados denominada *nós*. A DLT promete aumentar a eficiência e a transparência das colaborações entre indivíduos e/ou organizações com base em qualidades inerentes, como resistência à violação, à censura e democratização de dados.

No uso de aplicações estruturadas em *DLT* é preciso considerar a ideia de ambientes *não-confiável* sobre a influência das *falhas bizantinas*. Em LESLIE *et. al.* (1982), essas falhas ocorrem em situações em que as estruturas de nós estejam travadas ou inacessíveis, ainda que de modo temporária, em função de atrasos na rede, resultando em comportamentos maliciosos do nós quanto a emissão de informações incorretas. A vantagem no uso da estrutura *DLT* está na forma de armazenar as informações, seguindo um padrão ordenado e cronológico das informações, permitindo a cada transação a geração de metadados – *endereço do receptor, carimbos de data e hora* – cuja representação se assemelha a de um *ativo digital*.

Em HOUTAN *et. al.* (2020), o *blockchain* é um tipo de *DLT*, atuando de modo descentralizado, em rede e sem depender de qualquer autoridade central confiável, já que os *nós* participantes precisam alcançar o *consenso* sobre os *estados* dos dados transacionais para obter *confiança*. A arquitetura de uma rede *blockchain* pode ser vista na *Figura 17*, cuja ideia originalmente foi apresentada por NAKAMOTO (2008), fundamentando o conceito de *livro-razão* o qual é mantido pelas entidades/nós da rede. À medida que cada entidade armazena uma cópia do *livro-razão*, as origens dos dados podem ser verificadas nas transações realizadas por todos os entes envolvidos.

Dessa forma, a cadeia de blocos pode ser entendida como uma lista de registros ou de

blocos em constante crescimento. Os blocos são recipientes para armazenar transações, *pacotes identificáveis* carregando estados e históricos das mudanças dos dados. No entanto, cada bloco pode ser visto e *auditado* por qualquer ente da cadeia, favorecendo a *confiabilidade* e a *segurança* das transações. O contexto da aplicação baseia-se em um ambiente, onde busca-se garantir que a informação transitada seja *fidedigna*, seguindo o exemplo de assegurar como verdadeira a *identidade digital* de um determinado usuário. Em MUHLE *et.al*. (2018) a procura por métodos que assegure a fidedignidade dos dados com a finalidade de auxiliar o *gerenciamento de identidades digitais* aumentou em função do maior interesse da interação entre pessoas e serviços digitais.

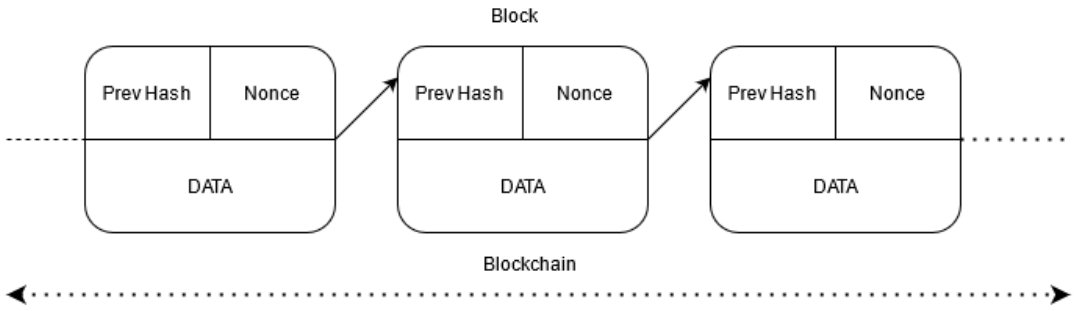

Figura 17. A arquitetura blockchain baseada orinalmente na ideia apresentada por NAKAMOTO (2008)

Os blocos criados, servem, portanto, como *registros de transações* vinculadas por meio de chaves *hashes*. Como não há um único ponto de controle para uma rede *blockchain*, ela pode ser considerada uma rede totalmente *descentralizada*. Assim, com base no conceito de *livro-razão*, a ideia de uso de *blockchain* em conjunto com o modelo de *identidade digital* é fortalecer e garantir a *imutabilidade dos dados*, ou seja, dar a garantia da autenticidade das informações, assegurando que elas não foram alteradas para favorecer um ou outro usuário durante a transação.

4.2 Propriedades

Um blockchain apresenta propriedades que o torna adequado em aplicações que demandam a *segurança* e a *garantia de dados fidedignos*. FERDOUS *et. al.* (2019) e GILANI *et. al.* (2020), apresentam as principais propriedades e características de um blockchain no contexto das *aplicações distribuídas*:

I. *Nós e blocos*: o *nó* é o computador numa rede *P2P* que representa o proprietário das

transações realizadas por determinado usuário. O *bloco* é uma estrutura imutável e distribuída no blockchain. Depois de obter consentimento da transação, o bloco é adicionado ao blockchain.

II. *Consenso distribuído*: A capacidade de alcançar um *consenso distribuído* sobre o estado do *Ledger* sem depender de qualquer elemento, denominado de *terceira parte* (TTP). Isso abre oportunidades para a construção de sistemas em que os estados e as interações possam ser verificados por quaisquer entidades autorizadas.

III. *Imutabilidade e irreversibilidade*: Alcançar um consenso distribuído com a participação de um grande número de nós garante que o estado do *Ledger* se torne imutável e irreversível após um certo período.

IV. *Persistência de dados (transação)*: Os dados em um *Ledger* distribuído é armazenado de forma distribuída garantindo a persistência, enquanto houver nós participantes em uma rede *P2P*.

V. *Proveniência de dados*: O processo de armazenamento de dados em qualquer *Ledger* distribuído é facilitado por meio de um procedimento chamado de *transação*. Cada transação precisa ser assinada digitalmente usando criptografia de chave pública que garanta a *autenticidade da fonte de dados*. Além disso, combina-se a imutabilidade e irreversibilidade dos dados dentro do *Ledger*.

VI. *Controle dos dados*: um *Ledger distribuído* garante que o controle sobre os dados, no armazenamento ou na recuperação, possa ser realizado de forma distribuída ainda que ocorram pontos de falhas.

VII. *Responsabilidade e transparência*: o estado do *Ledger* em conjunto com cada interação dos entes participantes pode ser verificado de forma distinta por qualquer entidade como um método para garantir a responsabilidade e transparência dos dados.

4.3 Árvore de Merkle

A árvore *Merkle* atua como uma *função representativa* de uma rede *blockchain*, já que contém todas as transações do bloco. Em LIU *et. al.* (2020), a *estrutura de árvore* assume a forma de um contêiner, divididas entre *corpo do bloco*, que contém as transações inseridas e o *cabeçalho* inserido na raiz Merkle juntamente com os demais atributos do bloco. A *Figura 18* apresenta uma visão geral da árvore *Merkle*.

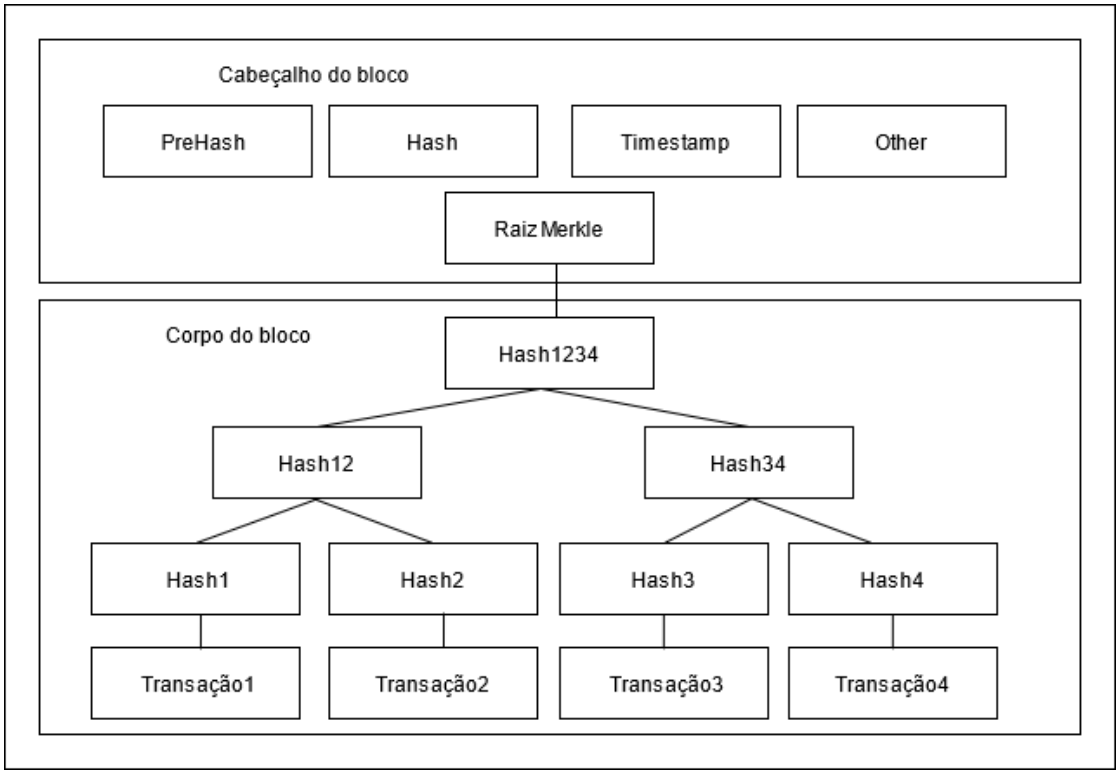

Figura 18. Representação de uma árvore de *Merkle* na cadeia de blocos. Adaptada de Liu et.al. (2020)

A árvore *Merkle* inclui o nó *raiz*, o *grupo de nós* internos e o *grupo de nós de folha*. Cada nó folha representa o *hash* da transação correspondente no bloco. O valor do nó interno é produzido e calculado no *hash* de dois nós filhos, e se houver apenas um filho, o *hash* será copiado. Desta forma, o nó raiz representará todas as transações, sendo o *hash* do nó raiz o identificador do bloco, onde estará tanto a chave pública como também a privada.

Em HOUTAN *et. al. (2020),* a estrutura de *Merkle* pode ser empregada para gerenciar o armazenamento e no controle de dados para garantir a acessibilidade dos conjuntos de chaves. Como os dados são convertidos em *hash,* apenas a raiz da árvore é armazenada no *blockchain*. Por outro lado, as chaves para acessar os dados pode ser armazenada nos dispositivos do usuário ou em algum outro sistema de armazenamento. A chave é gerada de forma que os dados fiquem criptografados, permitindo o acesso apenas para o proprietário que dispõe da chave privada, no contexto de um modelo de *criptografia assimétrica*.

4.4 Smart Contract

O conceito de *smart contract* surge como um protocolo projetado para *facilitar*, *validar* ou *fazer cumprir digitalmente* uma *negociação* ou a *execução* de um contrato. O conceito foi apresentado inicialmente em SZABO (1996), com a ideia de facilitar atividades comerciais

seguras na realização de aplicações complexas. A ideia é permitir transações automatizadas sem a necessidade de supervisão de uma entidade externa, como bancos, tribunais ou departamentos de serviços de saúde. A *Figura 19* ilustra a estrutura básica de um *smart contract*. Para LIU *et. al.* (2020), o uso de *smart contract* fortalece três recursos do *blockchain*, a saber*: operação permanente*, *não-violação* e *transparência de dados*. Sendo a inserção dos dados na rede *blockchain* permanente, o *smart contract* uma vez implantado não pode ser modificado durante a execução do contrato.

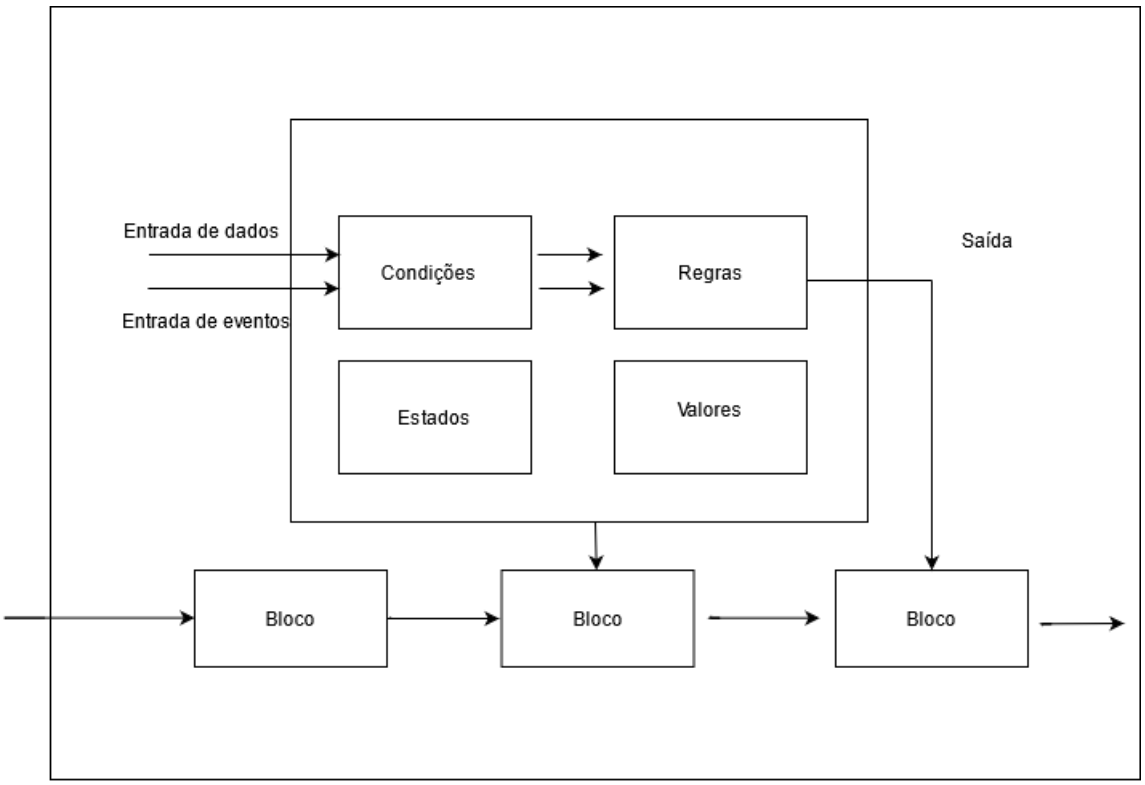

Figura 19. Estrutura de um *smart contract*. *LIU* et.al. *(2020)*

Em YANG *et. al. (2020),* mostra-se a implantação de um *smart contract* dentro da rede *blockchain*, a partir das regras e condições estabelecidas entre os entes envolvidos, a execução dos códigos segue de modo automático, já que não existe recursos de aceitação e de dependência de quaisquer intermediários. Os *contratos* são utilizados no envio de transações entre os entes, objetivando a *não-violação* de forma *unilateral* das regras.

O uso de *smart contract* permite que entidades tornem pública as operações realizadas, visando fortalecer o *método de consenso* dentro da rede *blockchain,* e com isso garantir a exatidão e a consistência dos resultados da transação.

4.5 Tipos de arquiteturas

Na concepção de uma rede Blockchain, os *tipos de arquiteturas* existentes predominantes seguem um padrão de implantação do tipo público, privado ou junção de ambos.

Em FERDOUS *et. al.* (2019), NASCIMENTO *et. al.* (2019) e HOUTAN *et. al.* (2020) os tipos de cadeias de blocos são discutidos e classificados em:

I. *Blockchain público*: esse tipo permite a qualquer pessoa criar e validar blocos, bem como modificar o estado do *blockchain* de transações realizadas entre todas as entidades participantes. Isso significa que os estados do bloco em conjunto com todas as transações estão acessíveis a todos. No entanto, uma questão a ser considerada nessa abordagem, é que há pouco controle em relação a privacidade dos dados e das transações realizadas.

II. *Blockchain privado*: nessa abordagem a existência de uma permissão pode ser restrita a contraparte pública no sentido de que apenas entidades autorizadas e confiáveis podem participar das atividades dentro do bloco. Ao permitir que apenas entidades autorizadas participem de atividades dentro do *blockchain*, a iniciativa é fortalecer e garantir a privacidade dos dados, o que pode ser desejável em alguns casos de uso.

III. *Blockchain híbrido:* o tipo representa a junção entre a abordagem privada e pública, em função da necessidade de integração entre as soluções, buscando uma maior interoperabilidade em grande escala. É, portanto, a combinação de tipos de soluções de rede, sendo uma uma cadeia de blocos centralizada, que é independente, porém pode se comunicar com outras redes, denominada cadeia chamada de rede pública

Uma outra classificação encontrada na literatura a despeito dos tipos de *blockchain* está entre exigir ou não uma *permissão* para que o bloco seja alterado. Em KANNENGIESSER *et. al.* (2019), no *tipo privado*, os nós do bloco podem ter a mesma permissão ou devem primeiro receber uma permissão para validar e confirmar novos dados, geralmente os dois ao mesmo tempo. Por outro lado, no *tipo público* não há a necessidade de permissão para alterar o bloco.

Em NASCIMENTO *et. al.* (2019), nós conduzimos uma revisão da literatura, que permitiu estruturar os principais tipos de *arquiteturas blockchain*, bem como enumerar as *características* encontradas, tipo de *controle* e formas de *armazenamento* aplicadas *no contexto de serviços públicos*, cf. a *Figura 20*.

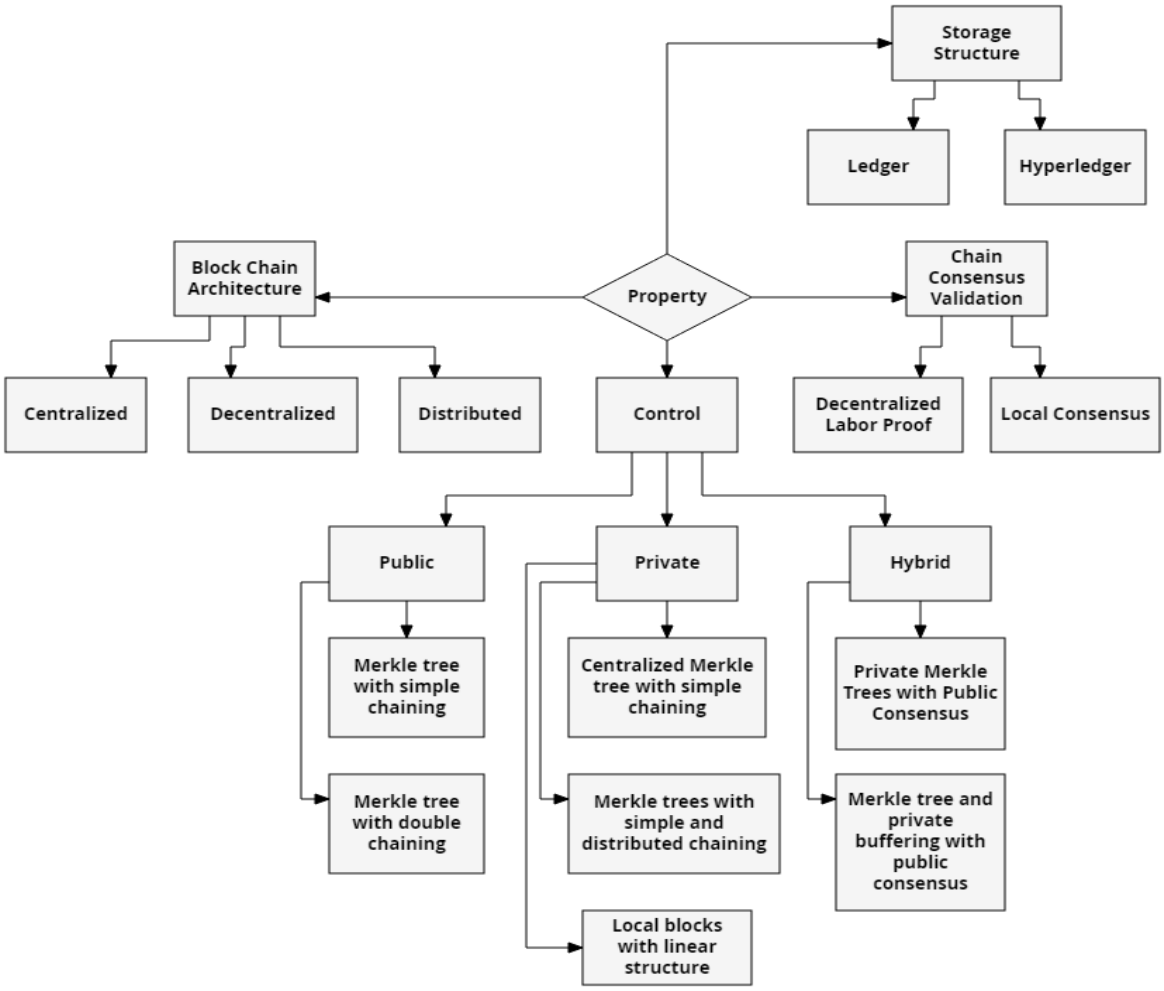

Figura 20. Modelos de arquiteturas e propriedades do *blockchain*. NASCIMENTO *et. al.* (2019)

De modo distinto, a organização da cadeia de blocos apresentada em NASCIMENTO *et. al*. (2019) é estruturada de três formas: centralizada, descentralizada e distribuída. Na forma *centralizada* a cadeia de blocos permanece armazenada em modo privado, os dados armazenados não dispõem de *consenso público* da rede *blockchain*, já que o *Ledger* envolvido também é centralizado e assim não é compartilhado com outro agente. Em seguida, na forma *distribuída* ou *pública* os dados estão distribuídos em vários servidores ou *nós*, a estrutura de consenso é criada em torno de tais servidores. Os *ledgers* podem ser compartilhados de acordo com o desejo dos agentes envolvidos, por meio, por exemplo, do uso de *smart contract*. Por fim, na estrutura *híbrida* há duas cadeias de blocos, a cadeia de blocos *centralizada*, denominada de *independente* ou rede *doméstica* e outra cadeia chamada de rede *pública*.

4.6 Soluções baseadas no modelo *Auto Soberano* de identidade

As soluções baseadas em *blockchain* utilizam diferentes tipos de gerenciamento de identidades. Por exemplo, como mostrado na *Figura 20,* escolhido o *tipo de cadeia* de blocos pública, um novo identificador é criado para cada correspondente pares de chaves públicas e privada, a partir do *hash*. Nesse sentido, o uso da tecnologia *blockchain* apresenta propriedades que fundamenta os métodos desejáveis para serem aplicados em conjunto com o modelo de identidade *Auto Soberana*. O *blockchain* fornece essencialmente um domínio *descentralizado* que não é controlado por nenhuma entidade particular, e em relação aos dados, esses últimos estarão armazenados em quaisquer *blockchain*, prontamente disponíveis para qualquer entidade autorizada.

A implementação de uma solução *blockchain* em conjunto com o modelo de identidade *Auto Soberana* fortalece o uso de aplicações de vários tipos, a exemplo: aplicações financeiras, saúde, compra e venda de bens, etc. No entanto, é preciso considerar alguns requisitos necessários para que essas aplicações sejam *moduláveis* e *interoperável*. Em *German Blockchain Association* (2018) as aplicações reúnem os seguintes componentes:

I. *Cliente-servidor*: os blocos de construção são totalmente controlados pelo proprietário da identidade. As aplicações clientes podem ser aplicativos de celular ou *web*, podendo os dados pessoais estarem armazenadas na nuvem ou em hardware específico de armazenamento. Porém, a ideia é de que apenas o proprietário dos dados tenha a posse do controle.
II. *Aplicações distribuídas*: são inerentes ao conceito do modelo de identidade digital *Auto Soberana*. Esse ponto faz intersecção com as características das aplicações baseadas em *blockchain* em relação a *acessibilidade* e a *legibilidade* na rede.
III. *Criação de chaves baseadas em criptografia*: é a camada fundamental do modelo de identidade digital *Auto Soberana*, responsável pela criação de uma identidade digital e pelo controle total do proprietário da identidade.
IV. *Gerenciamento de chaves:* é a função utilizada para gerenciar as chaves criptográficas criadas.
V. *Registro de identificador* (DID): é a camada que permite criar e registrar identificadores com base nas chaves de criptografia. Além disso, permite a revogação de um DID ou dos identificadores conectados.

VI. *Armazenagem*: é a camada onde o cliente armazena os atributos da identidade do proprietário como também outras credenciais verificadas. Serve como um cofre seguro e controlado pelo próprio proprietário da identidade.

Na *Figura 21* é apresentado um exemplo de arquitetura do modelo de identidade digital *Auto Soberana* quando vista pela perspectiva do *cliente*, ou do *proprietário* da identidade em uma rede descentralizada. Como já dito, a arquitetura em formato de blocos é característica fundamental do modelo de identidade *Auto Soberana*, ela representa a dimensão vista pelo lado do *cliente* quando ocorre a transação em uma rede distribuída.

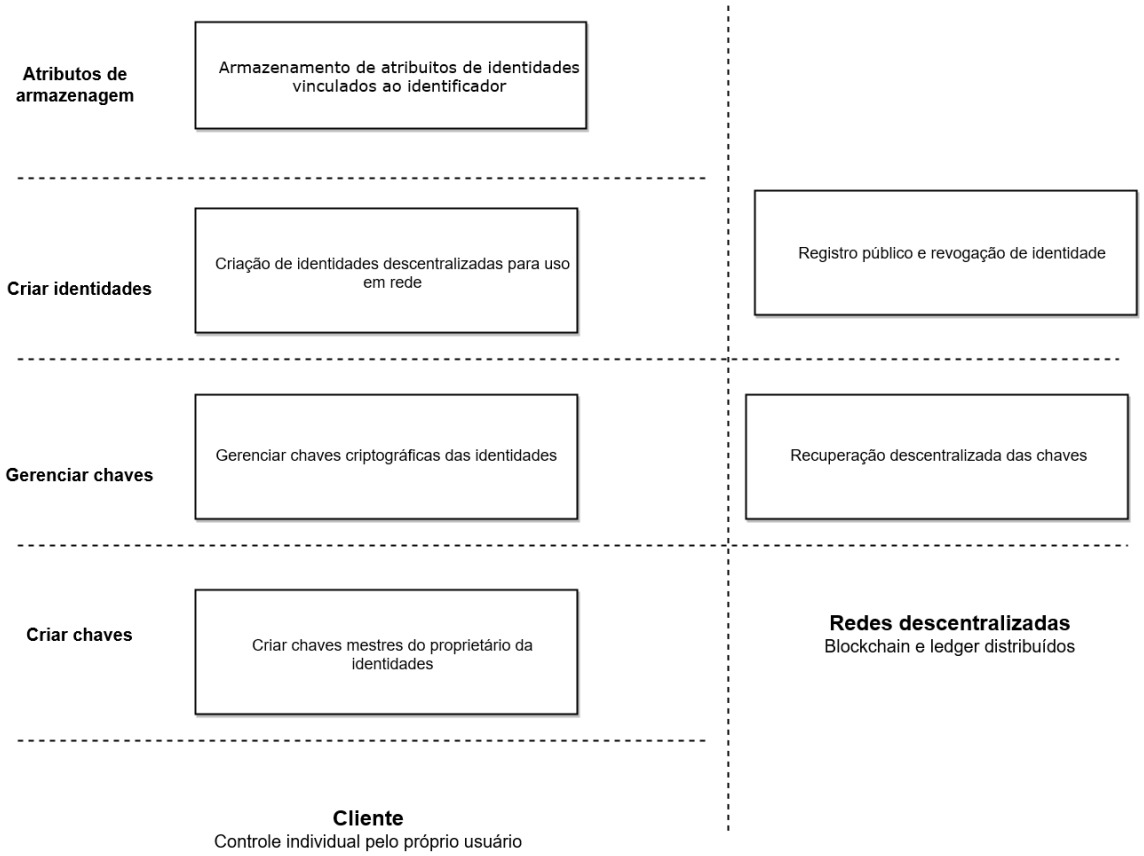

Figura 21. Arquitetura para identidade *Auto Soberana* com base em aplicações *blockchain*. Adaptada de *German Blockchain Association* (2018).

Os dados da identidade pertencem ao grupo de informações de identificação pessoal tal como ocorre na plataforma *blockchain* e é suportado por um *smart contract* que permite ao usuário criar controles de acesso para o compartilhamento de tais dados. Além disso, as propriedades de *imutabilidade de dados*, *controle distribuído*, *responsabilidade* e *transparência* fornecem uma base sólida sobre "como se pode implantar tais métodos para gerenciar identidades", fortalecendo assim a criação de aplicações cuja base apoia-se no

modelo de identidade *Auto Soberana*.

4.6.1 Comparativo das aplicações por tipo de arquitetura

Em NAIK *et. al.* (2019), DIB *et.al.* (2020), LIU *et. al.* (2020) e GILANI *et. al.* (2020) organizou-se a *Tabela 4* que representa um comparativo entre as *soluções* encontradas na literatura especializada, quanto ao uso ou aplicação do modelo de identidade *Auto Soberana*, como também demais características.

Tabela 4. Aplicações baseadas no modelo *Auto Soberano* de identidade. Adaptada de NAIK et. al. (2019), DIB et.al. (2020), LIU et. al. (2020) e GILANI et. al. (2020).

Soluções	**Ledger**	**Blockchain**	**Gerenciamento de Chaves**	**Storage (On / Off)**	**Divulgação seletiva**	***Smart Contract***
Sovrin[2]	Indy	Público	DPKI	Dentro / fora do *Ledger*	Sim	Sim
uPort[3]	Ethereum	Público	Dispositivo do usuário e DPKI	Fora do *Ledger*	Sim	Sim
ShoCard[4]	Bitcoin	Público	DPKI	Fora do *Ledger*	Não	Sim
Civic[5]	Ethereum	Público	Carteira digital	Dentro / fora do *Ledger*	Sim	Sim
Jolocom[6]	Ethereum	Hibrido	Chaves HD	Dentro / fora do *Ledger*	Sim	Sim
EverID[7]	Ethereum	Privado	Carteira digital / Biometria	Dentro / fora do *Ledger*	Sim	Sim

A *Tabela 4* apresenta as soluções sem nenhuma escala de avaliação definitiva, por isso são avaliadas e comparadas com outras soluções baseadas na *lei de identidade digital* apresenta por CAMERON (2005) e da *taxonomia* de identidade *Auto Soberana* apresentada na *Figura 9.* Aqui, o nosso objetivo é destacar os projetos baseados na implementação de *blockchain* em conjunto com o modelo de identidade digital *Auto Soberana*.

Em relação aos *atributos* que foram apresentados na avaliação das aplicações, as *características* observadas seguiram em especial um *tipo de blockchain* em conjunto com um

[2] Sovrin: https://sovrin.org
[3] *uPort: www.uport.me*
[4] *ShoCard: www.shocard.com*
[5] *Civic: www.civic.com*
[6] *Jolocom: https://jolocom.io/*
[7] *EverID: www.everest.org/*

tipo do *Ledger*. Para o *gerenciamento* das *chaves públicas* ou *privadas,* as aplicações mais encontradas foram dos tipos *DPKI, DKM e HD, assim* como o uso da estrutura de *carteira digital.*

4.6.2 uPort

A *uPort* é uma solução de *código aberto.* Ela permite os próprios usuários criarem uma identidade digital na rede *Ethereum*, assim como enviar e solicitar credenciais, assinar transações, e gerenciar com segurança chaves públicas e privadas dos respectivos dados. No aplicativo móvel da *uPort,* há a geração de pares de chaves que dá subsídio para a implantação de três *smart contract*. O primeiro *smart contract* é do tipo *proxy* onde será implantado o *identificador único* do usuário. Em seguida outro contrato é criado com a função de *controlador* para fornecer acesso de identidade e por fim, há o *smart contract* com a função de *registro* e de *recuperação* da identidade do usuário caso ele perca o acesso a ela. Na opção *uPort registry* há o vínculo da criptografia de dados de perfil ou de atributos para um identificador. A *Figura 22* representa a arquitetura da *uPort* com as respectivas funções.

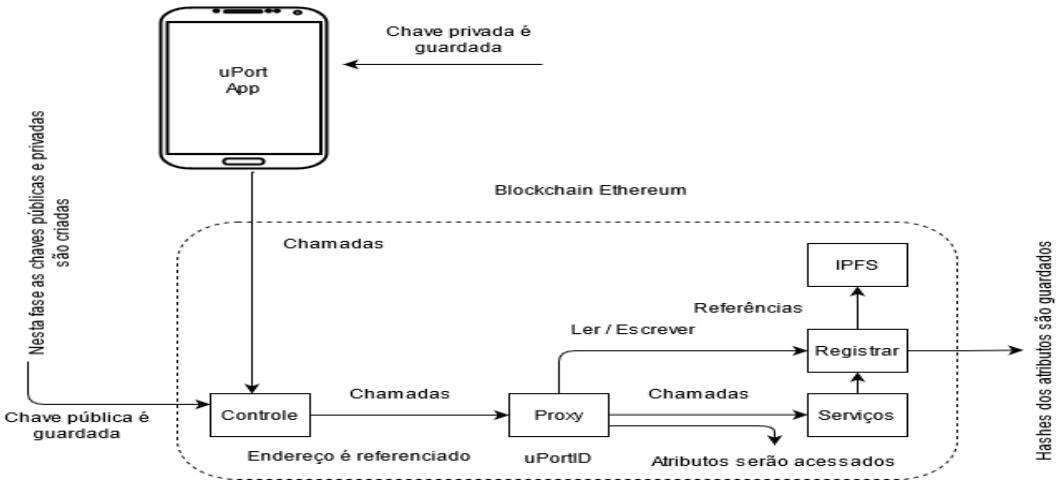

Figura 22. Arquitetura da uPort com os componentes da aplicação. Adaptado de FERDOUS *et. al.* (2019)

Para FERDOUS *et. al.* (2019), na *uPort* a maior parte dos dados de identidade são armazenados no formado de arquivos distribuídos *(IPFS),* em que o aplicativo móvel é utilizado apenas para armazenar a chave privada da correspondente identidade. O registro público é usado para criar uma correlação entre uma identidade *uPort* e dados do usuário no *IPFS.*

4.6.3 Sovrin

A *Sovrin* é uma fundação cuja missão é estabelecer padrões para possibilitar a criação da infraestrutura necessária para as identidades *Auto Soberana*, com o uso de *blockchain* para o armazenamento distribuído das identidades. Para STYBALDY *et. al.* (2020), o modelo de identidade *Auto Soberana* da Sovrin não depende de qualquer distribuição em particular, podendo operar em qualquer *blockchain* que atenda às propriedades exigidas. Ela é uma das propostas cuja a relação de confiança é estabelecida por meio de *credenciais verificáveis*. A solução foi criada no formato de código-fonte aberto e transferido para a *Linux Foundation* dando origem ao projeto *Hyperledger Indy*.

Em FERDOUS *et. al.* (2019), após a verificação das *credencias*, os usuários podem verificar a identidade de si mesmo, como também reivindicar a validação da identidade de outro usuário e/ ou de uma organização. Nesse sentido, a proposta busca permitir que os usuários exerçam o controle sobre a escolha de quais dados desejam compartilhar com outra pessoa. A *Figura 23*, apresenta a arquitetura da Sovrin com os componentes da aplicação.

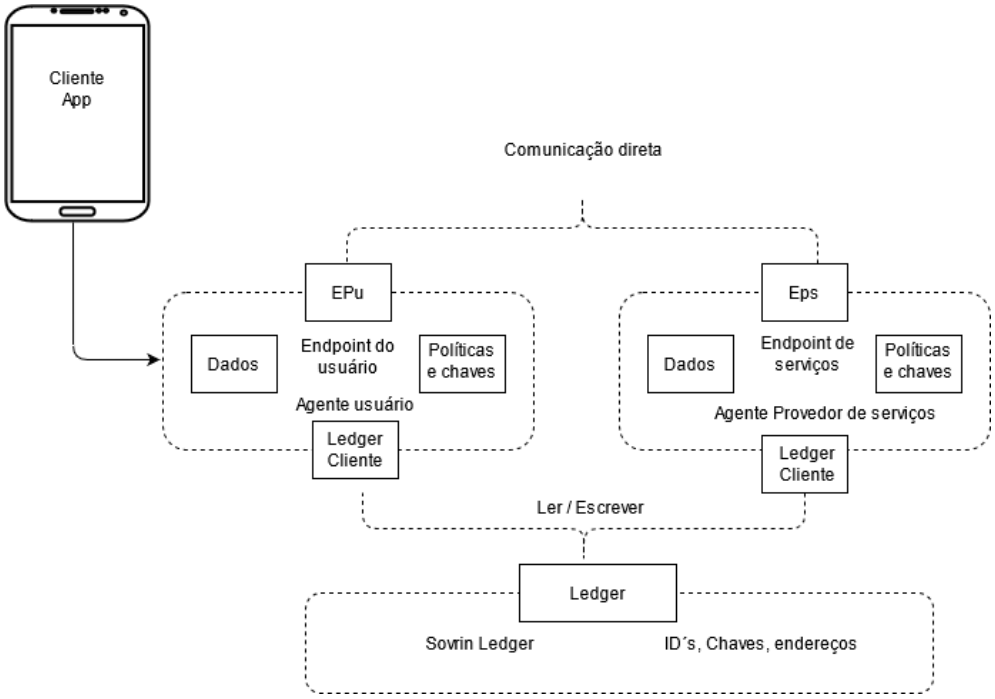

Figura 23. Arquitetura da Sovrin com os componentes da aplicação. Adaptado de FERDOUS *et. al.* (2019)

4.6.4 Jolocom

Em FERDOUS *et. al.* (2019) a *Jolocom* é outro sistema de identidade *Auto Soberana* cuja funcionalidade é semelhante ao *uPort*. Como a *uPort*, *ele* foi desenvolvido sobre a rede

Ethereum, assumindo a forma de vários *smart contract* dentro da *Ethereum*. Os usuários utilizam um aplicativo móvel, semelhante ao uPort, para interagir, criar, gerenciar e compartilhar suas identidades. A diferença da solução da *Jocolom* está na forma que os dados da identidade são estruturados e representados.

4.6.5 ShoCard

Em BOKKEM *et. al.* (2019), a plataforma de gerenciamento de identidade *ShoCard* é implementado usando *blockchain* e consiste de três funções principais: *autenticação* do indivíduo ou da entidade, e as trocas de *autorizações* e *atestados*. A existência da identidade do usuário é obtida a partir de um número de telefone ou de um documento oficial, por exemplo, um passaporte ou uma outra informação biométrica. O usuário tem o controle sobre os seus próprios dados, podendo esses dados serem armazenados localmente, no entanto, as chaves de verificação podem estar armazenadas de modo público na rede *blockchain*. Apenas o usuário pode optar por compartilhar os dados, o que significa que o *acesso* é uma das propriedades da aplicação. Os algoritmos são documentados no formato de código aberto e é independente do tipo de *blockchain*, fortalecendo, assim o atributo de *transparência*.

Em DIB *et. al.* (2020), os dados também são gravados em um *Ledger* para permitir a validação de dados a *posteriori*. O identificador da transação resultante é o *ShoCardID* do usuário e ele é armazenado em um dispositivo móvel com o certificado autenticado da aplicação. Para associar certificados a um *ShoCardID*, o usuário interage com um provedor de identidade por meio de um processo denominado *Certificação*. Embora inicialmente a solução utilize a rede do *Bitcoin*, ela é capaz de trabalhar em diferentes *blockchains*, já que a identidade da pessoa pode permanecer válida mesmo se algum *blockchain* parar de funcionar. Por isso a plataforma também é *persistente* em relação a *proteção* e está *presente* em função do uso de uma rede distribuída *blockchain*.

4.6.6 EverID

BOKKEM et. al. (2019), a aplicação *EverID* de modo contrário a solução *uPort*, o sistema descentralizado é usado para *armazena*r e *confirmar* os dados de identidade do usuário. A solução facilita a verificação de usuários por vários entes terceiros, permitindo a transferência segura de valor entre os membros da rede. Isso significa que as reivindicações feitas pelos usuários são demonstráveis. A arquitetura descentralizada da plataforma também fornece *propriedade* de dados pessoais que só podem ser acessados pelo usuário. Os dados do

indivíduo são registrados de tal maneira que permite ao indivíduo controlar *como* os dados são compartilhados, *com quem* e *por quanto* tempo (*persistência*). Este procedimento de compartilhamento é aplicado por meio de um *smart contract.* A infraestrutura *EverID* é executada em uma série de *nós* na rede, hospedeiros do *blockchain*, permitindo os indivíduos transferirem os dados para o aplicativo.

Isso torna a aplicação portátil, atuando de forma diferente das demais soluções, já que não é necessário ter um dispositivo para armazenamento local, pois a *identidade digital*—combinação de biometria, identificação governamental e confirmações de terceiros—pode ser armazenada na nuvem. No entanto, o *EverID* não atende à propriedade da *minimização*, isto é, quando os dados do usuário são solicitados para serem verificados, o usuário divulga os dados específicos na sua totalidade. Por exemplo, se há o interesse em saber se o usuário tem mais de 18 anos, o usuário pode optar por divulgar sua data de nascimento completa ou não. *EverID* é uma *solução privada*, embora ela seja uma solução baseada em *blockchain*, não é possível concluir que a propriedade da *transparência* baseado no modelo *Auto Soberano* de identidade é aplicada.

4.6.7 Civic

Em STYBALDY et. al. (2020), *Civic* é onde os pares de chaves são gerados a partir de uma *carteira digital*, permitindo que as informações sobre a identidade sejam armazenadas no dispositivo do usuário. O aplicativo e o *blockchain* só recebem *hashes* dos dados e os armazena como um *token* do tipo *ERC20* na rede *Ethereum*. A rede *Civic* acomoda de modo interdependente três entidades: *usuários*, *validadores* e *provedores de serviços*.

O *usuário* é qualquer pessoa que deseja usar o protocolo para registrar uma identidade. *Validadores* são responsáveis por verificar a autenticidade de uma identidade no *Ledger* distribuído. Essa entidade pode vender informações para *provedores de serviços* que precisam verificar as identidades de seus clientes; ele operacionaliza esse serviço por meio da troca de dados usando *token Civic* (*CVC*). O *CVC* é utilizado como uma forma de liquidação entre as partes de uma transação relacionada à identidade dentro de um ecossistema. Uma aplicação *Civic* é construída sobre a rede *blockchain Ethereum* com uso de *smart contract* para colocar em prática o atestado de dados e de pagamentos por este trabalho.

4.6.8 Aplicações no contexto da taxonomia do modelo *Auto Soberano*

Em relação as aplicações, em BOKKEM *et. al.* (2019), FERDOUS *et. al.* (2019), NAIK *et. al.* (2019), STYBALDY *et. al.* (2020) e GILANI *et. al.* (2020), a *Tabela 5* e em conjunto com a *taxonomia* vista na *Figura 9*, indica a presença ou não das *propriedades* que compõem o modelo Auto Soberano de Identidade digital para cada solução: *UPort, Sovrin, Jolom, Civic, ShoCard e EverID.*

Tabela 5. Aplicações baseadas em *blockchain* em conjunto com a taxonomia do modelo de identidade *Auto Soberano*, com os critérios que são satisfeitos (✓) e os que não são (●).

Taxonomia / Tipos de Soluções		**uPort**	**Sovrin**	**Jolom**	**Civic**	**ShoCard**	**EverID**
Fundamentos	Existência	✓	✓	✓	✓	✓	✓
	Autonomia	●	✓	●	✓	✓	✓
	Acesso	✓	✓	✓	✓	✓	✓
	Fonte único	●	●	●	✓	✓	✓
Segurança	Proteção	●	✓	✓	●	✓	✓
	Disponibilidade	✓	✓	✓	✓	✓	✓
	Persistência	✓	✓	✓	✓	✓	✓
Controle	Capacidade de escolha	✓	✓	●	✓	✓	✓
	Divulgação	✓	✓	●	✓	✓	✓
	Consentimento	✓	✓	●	✓	✓	✓
Flexibilidade	Portabilidade	●	●	●	●	✓	✓
	Interoperabilidade	●	●	●	✓	✓	✓
	Minimização	✓	●	●	✓	✓	●
Sustentabilidade	Transparência	✓	✓	✓	✓	✓	●
	Padrão	✓	✓	✓	✓	✓	✓
	Custo	✓	✓	✓	✓	✓	✓

4.7 As leis de proteção dos dados no modelo *Auto Soberano* de *Identidade Digital*

Nas aplicações *web* que atuam de modo descentralizado não há um controle sobre os dados que seja suficientemente forte para evitar os casos de violações do ponto de vista da privacidade do usuário, conforme apresentado no *Capítulo 02*. No entanto, empresas e organizações quando utilizam de dados de usuários na execução de seus próprios modelos de negócios, necessitam cumprir uma série de orientações que constam nas leis sobre proteção dos dados. Em CANEDO *et. al.* (2020) a proteção de dados pessoais é um assunto abordado

em vários países, onde muitas leis foram aprovadas e já estão em vigor. Como exemplo, temos: o *Regulamento Geral de Proteção de Dados* (GDPR), a *Lei sobre a Proteção de Informações Pessoais* (APPI), os *Princípios* de *Privacidade Australianos* (APPs), a *Lei de Proteção de Informações Pessoais e Documentos Electrónicos* (PIPEDA) e as leis dos Estados Unidos, incluindo a *Lei de Privacidade do Consumidor da Califórnia de 2018* (CCPA). Para esse trabalho, em especial será vista a *GDPR* no caso europeu e a *Lei Geral de Proteção aos Dados* (LGPD) — Lei nº 13.709 / 2018—, no caso brasileiro.

Para este estudo, entende-se como necessário o uso de métodos que possa garantir a segurança sobre o *uso dos dados* tanto do lado do *usuário-cliente* quanto da *organização* ou *empresa*. Entende-se, também, no cenário das aplicações, uma oportunidade para incentivar o uso do *modelo Auto Soberano* de *identidade digital* como instrumento para garantir o *compartilhamento proativo* e do *consentimento de uso dos dados*.

4.7.1 As leis de proteção dos dados

Na perspectiva de trabalhos acadêmicos dentro da abordagem da *engenharia de software* ainda há poucos casos práticos—ou na literatura—que abordem a criação de soluções que se basearam na LGPD. Por outro lado, na aplicação da GDPR em conjunto para a construção de sistemas SILVA *et. al.* (2019) apresenta iniciativas que seguiram os princípios do GDPR, em especial, para o *design de software*. Nessa mesma linha, NAIK *et. al.* (2020) mostra um estudo como um caso da aplicação do *modelo Auto Soberano de identidade* em conjunto com as regras da GDPR. Segundo CANEDO *et. al.* (2020), tanto a LGPD quanto a GDPR foram baseadas na *ISO / IEC 27701*, norma essa que especifica as técnicas de segurança para gerenciamento de informações e da privacidade dos dados.

4.7.1.1 A Regulamento Geral de Proteção aos Dados

O GDPR surgiu como instrumento normativo para regulamentar o tratamento de dados pessoais, bem como as regras de compartilhamento desses dados. O objetivo desta regulamentação é proteger os direitos e liberdades fundamentais das pessoas físicas em relação à proteção de seus dados.

Em CANEDO et. al. (2020), o normativo GDPR refere-se ao *processamento total* ou *parcial de dados pessoais* por meios *automatizados* e *não automatizados*. Dessa forma, para garantir a segurança e a privacidade dos dados pessoais, o GDPR apresenta os deveres e obrigações do controlador e do processador de dados pessoais. Assim, com base no

normativo, o *controlador* é grupo formado por pessoas ou por autoridades públicas que de forma isolada ou em conjunto determinam os propósitos e meios para o processamento de dados pessoais. Na outra ponta, está o *processador*, pessoa física ou jurídica cuja responsabilidade é a de processar dados pessoais em nome do controlador.

Para IRAMINA (2020), os benefícios da implementação das diretrizes trazidas pela GDPR atuaram no sentido do fortalecimento dos *direitos dos indivíduos sobre seus dados*, encerram a maior responsabilidade para empresas em relação aos dados pessoais coletados, com também em sanções mais severas para aquelas que não agirem em conformidade com as novas regras.

4.7.1.2 A Lei Geral de Proteção aos Dados

No caso brasileiro, a LGPD instituída por meio do ato normativo da Lei nº 13.709 / 2018, colocou o Brasil entre os países que possuem uma lei de *proteção de dados pessoais*. O normativo se aplica a indivíduos, empresas e órgãos públicos do país—independentemente do meio utilizado para processamento—, em que a sede da instituição esteja localizada e até mesmo no país em que os dados estejam localizados, desde que os dados processados sejam do tipo pessoal e originado no Brasil, cuja finalidade desta coleta tenha sido o fornecimento de bens e de serviços.

O *artigo 18 da* LGPD apresenta os direitos do indivíduo em relação a proteção de seus dados:

I. confirmação da existência de tratamento;
II. acesso aos dados;
III. correção de dados incompletos, inexatos ou desatualizados;
IV. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados sem conformidade com o disposto nesta Lei;
V. portabilidade dos dados a outro fornecedor de serviços ou produtos, mediante requisição expressa e observados segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
VI. eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII. informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII. informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX. revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Em CANEDO et. al. (2020), na LGPD, os dados pessoais são quaisquer informações relacionadas a um indivíduo que podem ser identificados. Por outro lado, os dados anônimos

não são considerados dados pessoais, exceto quando o processo de anonimato pode ser revertido e a pessoa pode ser identificada por esses dados. Além disso, o *consentimento prévio do proprietário* é necessário para a transferência de dados pessoais entre entidades com as garantias adequadas de acordo com os *princípios e direitos do proprietário dos dados.*

4.7.2 Comparativo entre as leis de proteção dos dados e o modelo *Auto Soberano* de identidade

A LGPD como também o Regulamento Geral de Proteção de Dados são instrumentos normativos que visam proteger os dados pessoais e a livre circulação desses dados. Para CARVALHO *et. al.* (2020), no cenário brasileiro, muitas organizações têm considerado a ação de *anonimização* como uma solução milagrosa para resolver a proteção de dados e das questões de privacidade no ambiente de aplicações com uso de *Big Data*. Nesse sentido, nós apresentamos a seguir as características de tal ação e de como utilizá-la:

I. Para ser considerado anônimo, não deve ser possível identificar uma pessoa, mesmo com um perfil sem nome.
II. Um ponto a preocupar-se é a suposição sobre o que é considerado o dado identificado ou identificável para definir dados anônimos. De fato, mesmo na estrutura legal existe uma margem razoável para considerar os dados como anônimos, e no uso de quantidades maiores de recursos os dados anônimos podem ser re-identificados.
III. A identificação depende de critérios que mudam de acordo com os avanços técnicos ou mesmo pelas condições específicas de análise e isso pode causar incerteza em relação anonimização.
IV. Os dados anônimos, no contexto de uso em uma solução, por exemplo de *Big Data*, têm maior possibilidade de re-identificação já que tal solução lida normalmente com grandes massas de dados, cuja disponibilidade dos dados permite conexão de informações de modo mais fácil, mesmo que os dados estejam fragmentados.

Para NAIK *et. al.* (2020) o uso da GDPR só se aplica quando os dados pessoais são processados, logo não se aplicaria quando não há dados pessoais. Por outro lado, o modelo *Auto Soberano* está baseado na estrutura de *Ledger* distribuído e *blockchain* com várias possibilidades de arquitetura, em especial do tipo privado e público. No caso da aplicação do modelo *LGPD* em conjunto com o modelo *Auto Soberano* ainda não há casos práticos identificáveis. No entanto, em NAIK et. al. (2020) e com base nos normativos *GDPR* e *LGPD*

(cf. *Tabela 6*) procurou-se apresentar uma avaliação dos aspectos de *compatibilidade* e *incompatibilidade* de ambos normativos em conjunto com as características do modelo *Auto Soberano* de modo geral.

Tabela 6. A relação de requisitos da GDPR, LGPD e *Auto Soberano*. A presença da característica (✓) ou a ausência (●).

Requisitos	**GDPR**	**LGPD**	**Auto Soberano**
Legalidade, justiça e transparência	✓	✓	✓
Limitação de propósito	✓	✓	✓
Minimização de dados	✓	✓	✓
Acurácia	✓	✓	✓
Limitação de armazenamento	●	●	●
Integridade e confidencialidade	✓	✓	✓
Responsabilidade	✓	✓	●
Consentimento	✓	✓	✓
Transferência extraterritorial de dados	✓	✓	●
Terceirização do tratamento de dados	✓	✓	●
Impedimento no tratamento de dados pessoais de crianças e de adolescentes	✓	✓	●
Sanção em caso de descumprimento da lei	✓	✓	●

Como já dito, a Tabela 6 é uma análise comparativa em relação aos requisitos normativos encontrados tanto na GDPR e quanto da LGPD em comparação ao modelo *Auto Soberano*. Em termos de soluções práticas, em NAIK *et. al.* (2020) foi apresentado um comparativo das soluções da *uPort* e da *Sovrin* com os princípios do GDPR. Nesta análise comparativa identificou-se que o ecossistema da *uPort,* cuja base é um *blockchain* público é um desafio para cumprir as conformidades exigidas do GDPR.

No entanto, na solução da *Sovrin* que é baseada em um *blockchain* público, porém do tipo *Public-Permissioned* é capaz de cumprir os princípios da GDPR, pois o modelo de governança é operado por um consórcio de organizações confiáveis. Dessa forma, o que se vê é que no uso de soluções com base no modelo *Auto Soberano* em conjunto com as leis de proteção de dados, o tipo de arquitetura *blockchain* tem influência significativa positiva. Esta compatibilidade de uso pode ser aprimorada quando se usa um *blockchain* do *tipo privado* e com *permissão*. Porém, pode gerar conflitos com os princípios básicos do modelo *Auto Soberano* em relação a *soberania* e do *controle dos dados pessoais.*

4.8 Casos de usos e aplicações

Muitas soluções foram propostas e desenvolvidas a partir da perspectiva pessoal da *gestão de identidade digital*, da *segurança de dados* e da *privacidade*. Nesse estudo, limitou-se a discussão de *sistemas* e de *arquiteturas* que apresentaram o gerenciamento de identidade

digital e da privacidade de dados do usuário baseado em *blockchain* e no modelo de identidade *Auto Soberana*.

A exemplo, BANDARA *et. al.* (2021) apresentou uma plataforma de carteira digital para manter as identidades digitais em conjunto com os dados de locomoção do usuário em uma plataforma baseada em *blockchain* com o uso de provas de identidade *Auto Soberana* (SSI). A solução foi uma iniciativa para ajudar no enfrentamento da *COVID-19*. A *Figura 24* apresenta os recursos utilizados para o enfrentamento do desafio de operacionalização do *rastreamento digital* de passaportes de vacinas.

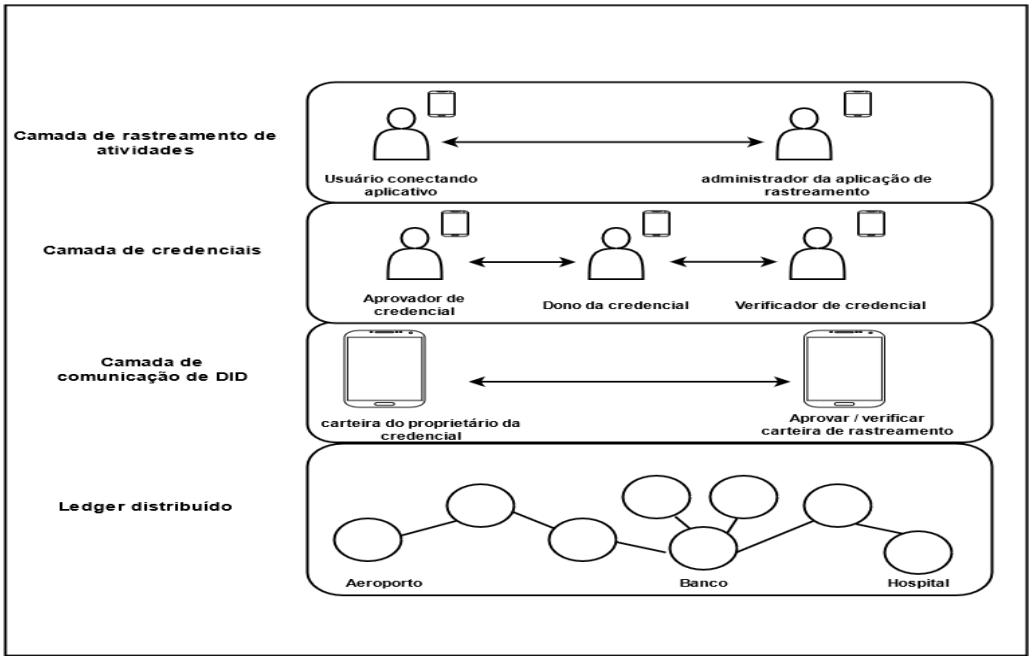

Figura 24. Recursos utilizados para o enfrentamento COVID-19 com base no rastreamento digital. Adaptado de BANDARA et. al. (2021).

Em relação a aplicação BANDARA *et. al.* (2021) avaliou-se o desempenho do armazenamento no *Ledger* da rede *blockchain* apresentando as seguintes contribuições:

I. A *plataforma de rastreamento* de digital foi habilitada para uso no enfrentamento para controle da COVID-19;

II. A *carteira de identidade*, no formato de aplicativo foi introduzida para capturar/verificar as provas de identidade do usuário e do *rastreamento das atividades de registro.*

III. Um procedimento para *armazenar dados da identidade* do usuário e dos dados das atividades de locomoção do usuário foi introduzido com o objetivo de rastrear por onde passou o usuário portador da *COVID-19*, utilizando os métodos da identidade *Auto Soberana* como provas fidedignas dos registros.

IV. A identidade *Auto Soberana*, baseada em prova de identidade e arquitetura para rastreio das atividades, foi apresentada para levar em conta as questões do armazenamento de dados em nuvem e em relação a *falta de privacidade*, da *ausência de imutabilida*de, da *rastreabilidade* e da *proveniência de dados*.

Nessa mesma linha, HASAN *et. al*. (2020) apresentou outra solução que implementa *passaportes médicos digitais* (DMP) com *certificados de imunidade* para os participantes do teste *COVID-19*. A contribuição da proposta está em utilizar um *blockchain* incorporando os métodos da identidade *Auto Soberana*, com uso de *proxies* de criptografia, armazenamento descentralizado e sistemas de arquivos interplanetários (IPFS) no formato de um documento de *passaporte pessoal*.

Nessa aplicação foi utilizado *smart contract* dentro da rede da *Ethereum* para manter uma identidade digital médica de pessoas com o objetivo de fornecer respostas rápidas, confiáveis a serem verificadas pelas autoridades médicas. Como resultado, a solução promoveu a redução no tempo de verificação de informações médicas, assim como um instrumento para enfrentar a disseminação de informações falsas, dado que as informações inseridas dentro do *Ledger* são confiáveis e imutáveis.

Em outro exemplo, dado o aumento da procura por serviços *online*, aumentou a necessidade de colocar em prática recursos mais eficazes em relação a *autenticação*, *autorização* para acessar tais serviços e para *controlar o gerenciamento de identidade* dos usuários. Nesse cenário, em AHMED *et. al.* (2020), relata-se vários problemas face ao uso de *repositórios fragmentados de identidade*, o que facilita roubo e violações de dados da identidade digital do usuário, em especial, quando segue-se modelos de identidade centralizada.

Por outro lado, como o modelo *Auto Soberano* de identidade devolve o controle sobre a identidade para o usuário, trazendo-o para o centro do modelo, a proposta pode ser aplicada no uso de serviços bancários, como forma de identificar chamadas fraudulentas de tais serviços e assim evitar as possíveis perda das contas pessoais. A solução foi baseada no uso da plataforma *Hyperledger Indy*, com objetivo de fortalecer o processo *conheça seu cliente* e assim aumentar a confiança de *agências delegadas* pelos bancos para entregar serviços financeiros.

SHETTY *et. al.* (2018) apresentou uma aplicação para gerenciar registros médicos cuja arquitetura foi desenvolvida com objetivo de preservar a *privacidade do usuário*. Nessa arquitetura, na camada de *compartilhamento de dados*, os usuários encerram o total *controle*

sobre dados pessoais de saúde, em especial, quando ocorre demandas de transações ou solicitações feitas por terceiros. Na camada de *hardware* é onde ocorre o fornecimento do ambiente para que ocorra a execução dos *hashes*, gerando *tokens* de acesso aos dados e do armazenamento dos dados confiáveis.

A ideia é ir além do fortalecimento da privacidade e ter a opção de revogar o acesso aos dados quando necessário. Em outras palavras, o *blockchain* é *camada da rede, distribuída* e *confiável*, que registra todas as operações, assim como as solicitações de acesso com o propósito de assegurar a *imutabilidade* e *integridade dos dados*. Esse cenário é ilustrado na *Figura 25* em uma aplicação centralizada no paciente. Os dispositivos do usuário coletam dados de saúde e os enviam de modo sincronizado para conta do usuário.

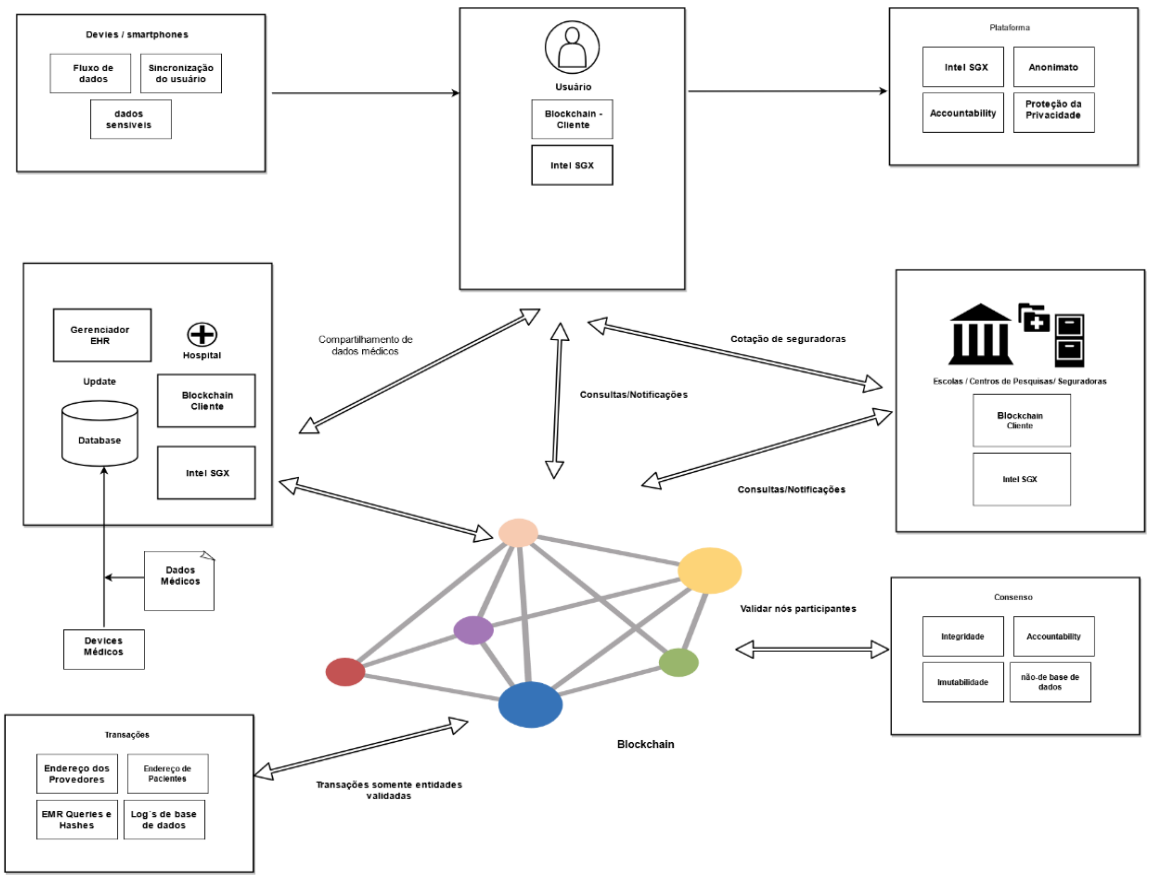

Figura 25. Aplicação de saúde centralizada no paciente. Adaptado de SHETTY *et. al.* (2018).

O dado de saúde contém um código *hash* que é carregado para a rede *blockchain* com a finalidade de garantir a integridade e a proteção dos registros. Os dados originais são mantidos na base de dados hospedada em uma plataforma em nuvem. O usuário tem o controle sobre os seus dados pessoais de saúde. São gerados *tokens* para conceder, negar ou revogar o acesso aos dados de qualquer outra parte da aplicação. Por exemplo, o usuário ao

procurar um tratamento médico, ele pode conceder ao médico escolhido um único *token* de acesso a dados. O mesmo exemplo pode ser aplicado à seguradora do plano de saúde, em que o usuário tem o poder para controlar as interações com outros agentes de negócio.

No quesito de registro de informações, o usuário pode registrar manualmente todas as atividades de acordo com o tratamento médico, a exemplo do uso de medicamentos. Essas informações são frequentemente compartilhadas com o médico. Do lado da aplicação, os prestadores de serviços de saúde podem solicitar exames clínicos e a verificação de tratamento anteriores. As solicitações de dados e os correspondentes acessos são registrados na rede *blockchain* para validação distribuída. Além disso, o usuário pode solicitar uma cotação de seguro-saúde às seguradoras e escolher planos de saúde disponíveis. As seguradoras, do mesmo modo, também podem solicitar acesso aos dados de saúde do usuário e os históricos médicos de tratamento.

Ao utilizar a tecnologia *blockchain*, quando aplicada, por exemplo, em sistemas de registros médicos, é possível distribuir a responsabilidade e garantir confiança nos dados, já que são imutáveis. Dito de outra forma, o modelo de identidade *Auto Soberana* permite trazer o usuário para o centro da arquitetura, dando a ele o poder de controle, de dar acesso e permissões sobre os seus dados. O controle baseado em *tokens* é a verificação utilizada para chancelar o acesso de informações do usuário quando solicitada por terceiros.

4.9 Agentes de software

Na literatura o conceito de agente no sentido etimológico da palavra assume o sentido de que alguém tem as capacidades necessárias para representar outra pessoa em dado uma situação. Por exemplo, um funcionário ou um empregado fica incumbido de representar ou de falar em nome da organização em atua, nesse caso funcionário é o agente representante da entidade. No entanto, no campo da ciência da computação definir com precisão a ideia em torno do conceito sobre o que é um agente não é tarefa tão simples, já que o conceito em assim assume definições diversas a depender do tipo de recurso que esse agente utiliza. Nesta seção, procurou-se apontar as principais definições, como também dos recursos envolvidos no tema.

Em RUSSELL *et. al.* (2013), um agente é definido como tudo o que pode ser considerado capaz de perceber seu ambiente por meio de *sensores* e de agir sobre esse ambiente por intermédio de atuadores. De modo semelhante, essa definição foi confirmada em pesquisas em VASILAKOS *et. al.* (2017). Por outro lado, SRINIVASAN *et. al.* (2010) apresenta uma perspectiva diferente no sentido de que um agente é um *sistema computacional*

encapsulado inserido em algum ambiente com a capacidade de atuar de forma *autônoma* a fim de atender o objetivo do projeto.

Nessa mesma abordagem, DORRI *et. al*. (2018) caracteriza o conceito de agente, como uma *entidade* que é inserida em um *ambiente* para detectar diferentes *parâmetros* para serem utilizados na *tomada de decisão* com base no *objetivo da entidade*. A entidade realiza a ação necessária sobre ambiente a partir desta decisão. Com base nessa definição compreende-se que:

1. *Entidade* - se traduz no tipo de agente, esse pode ser um software, como por exemplo um *daemon* de segurança, um componente de *hardware* do tipo termostato ou uma combinação de ambos como um *robô*.
2. *Ambiente* - entende-se como o local onde o agente está localizado, isso pode ser uma rede, a exemplo do uso em monitoramento de tráfego ou um software quando pretende-se monitorar comporatmentos de componentes de aplicações dentro de um sistema. Um agente utiliza as informações coletadas do ambiente para a tomada de decisões.
3. *Parâmetros* - os diferentes tipos de dados que um agente pode sentir a partir do ambiente são referidos como parâmetros. Por exemplo, os parâmetros para um agente-robô dentro de jogo os parâmetros são a posição, velocidades, e a posição dos elemenntos do jogo.
4. Ação – o agente pode executar uma ação que resulta em mudanças no ambiente, essas ações podem ser discretas ou contínuas. No conjunto de ações contínuas, o agente pode realizar ações ilimitadas. De modo contrário, nas ações discretas há um conjunto determinado de ações, a exemplo do agente controlador do termostato instalado em uma sala.

Em relação ao ambiente e dos recursos necessários para compor um sistema baseado em agentes temos em WOOLDRIDGE *et. al.* (2009):

I. *Acessibilidade*: é referente à precisão com o qual os agentes podem detectar dados do ambiente. Sendo o ambiente acessível, os agentes podem detectar dados precisos e atualizados sobre o ambiente. Por exemplo, em um firewall de rede o agente pode capturar todo o tráfego da rede.
II. *Determinismo*: se dá através da previsibilidade dos resultados da ação. No ambiente determinístico os resultados são previsíveis, já que o ambiente neste caso pode modelado a semelhança de uma máquina de estado, pois o agente conhece precisamente o próximo estado para cada ação. Por outro lado, em ambientes não-

determinísticos, o resultado da ação não é totalmente previsível não sendo influenciado por outros fatores, a exemplo de um jogo, o resultado depende das ações de todos os participantes.

I. *Dinamismo*: as mudanças que ocorrem no ambiente são independentes das ações tomadas pelos agentes. Se as mudanças nos ambiente são consequência da ação dos agentes este é considerado uma ambiemte estático. No geral, o ambiente é considerado dinâmico. O agente percebe a mudança no ambiente e realiza uma decisão dentro do processo.

II. *Continuidade*: Um *ambiente contínuo* afeta o estado do agente por meio de uma função contínua, a exemplo quando um agente se move dentro de um ambiente físico. Um ambiente discreto, por outro lado, restringe o agente a estar dentro de um conjunto de estados predeterminados, é o caso do agente móvel que mede sua posição e marca a data e a hora à medida que se move.

Para BRADSHAW (2012), o uso de agentes atende a políticas em *emergências coativas*, ou seja, a necessidade de criação da estratégia de *trabalho em equipe* para atingir o *objetivo*. Dito isso, o interesse no entendimento sobre *entidades autônomas* foca-se, primordialmente, para a *resolução de problemas*, de forma *cooperada* e/ou *coordenada*. Nessa lógica, o aparato conceitual sobre agentes fornece um conjunto poderoso e útil de estruturas e de processos para projetar e construir softwares complexos. Cada agente é um nó, com características intrínsecas, pelas quais tem o controle de modo local.

O agente de software também é denominado como um *agente inteligente*, essa característica encontrada em JENNINGS *et. al.* (1998) reforça a necessidade de os agentes de softwares serem *responsável, proativo e social*. A *responsabilidade* se traduz na função na qual os agentes devem atuar sobre o ambiente e responder de forma oportuna para as mudanças que ocorrem nele. A *proatividade* não é simplesmente agir em resposta aos estímulos do ambiente, mas é em ser capaz de exibir um comportamento oportunista, dirigido por objetivo e assumir a iniciativa quando apropriado. No atributo *social*, os agentes devem ser capazes de interagir, quando julgarem apropriado, com outros agentes para resolver o próprio problema e ajudar outros agentes na realização das tarefas.

Há ainda outras percepções que distinguem os agentes, por exemplo para BRENNER (1998) um agente requer uma certa dose de *inteligência* para executar as próprias tarefas. Sendo assim, pode-se classificar *agentes não-inteligente* como qualquer programa de software tradicional, já que esses apenas executam uma tarefa específica, a qual gera apenas economia de tempo para os usuários. No entanto, somente a inteligência permite ao agente a

execução de tarefa de forma autônoma, exigindo ou não a intervenção do usuário para decisões importantes. Os agentes são entes *racionais*, pois eles têm várias motivações, as quais se baseiam-se em objetivos, intenções ou desejos, que os ajudam a fazer escolhas em qualquer ponto da jornada.

Em FISHER (2009), essas motivações não apenas ajudam a direcionar as *escolhas* de um agente, mas podem criar, de modo dinâmico, novas motivações, adicionadas a qualquer tempo. Assim, se considerarmos, por exemplo, uma máquina de estado, ela fornece apenas algumas motivações, então pode-se evitar as sequências "ruins". Há, portanto, uma relação de complexidade entre os agentes e quando combinados entre si representam o conjunto das regras para as quais tem que seguir na execução do objetivo.

4.9.1 Classificação de Agentes

Há várias dimensões as quais pode-se classificar agentes. Para BRENNER *et. al*. (1998), os agentes de software podem ser classificados em função do tipo de tarefa à qual irá realizar. Nessa linha há agentes do tipo informação, de cooperação e de transação. O agente de informação tem como tarefa principal fornecer suporte ao usuário na busca por informações em sistemas distribuídos ou em redes. As principais tarefas é de ser capaz de localizar, extrair informações de fontes e filtrar com relevância o que se procura.

O agente de cooperação tem um foco diferente, já que tem como missão resolver problemas por meio de mecanismos de comunicação e de cooperação com outros agentes ou com outros recursos externos. Nesse quesito, a cooperação surge quando um problema excede as capacidades individual do agente ou quando já existem agentes que já tem solução a qual pode ser utilizado por outros agentes. Os agentes do tipo transação focam em realizar transações em ambientes orientados a serviços, a exemplo de ambientes de banco de dados, no monitoramento de sistemas de redes e no comércio eletrônico. A principal tarefa é garantir o processamento e monitoramento de transações.

De modo diferente, em JENNINGS *et. al.* (1998) os agentes de software podem ser classificados:

I. Em *função do tipo de mobilidade*, podendo ser do tipo estático ou móvel.

II. Em *função da tomada de decisão*, sendo *deliberativos ou reativos*. São deliberativos os agentes construídos com base no paradigma no qual os agentes possuem um modelo de raciocínio simbólico interno, e se envolvem no planejamento e na

negociação com outros agentes para atingir seus objetivos. No modelo reativo não existe nenhum modelo interno, e eles apenas agem ou respondem aos estímulos originados do ambiente.

III. Em *função dos atributos* que podem ou deve exibir. Nessa lista de atributos temos a autonomia, aprendizagem e a cooperação. A autonomia se baseia na ideia de que os agentes podem operar por conta própria, sem a necessidade de orientação humana ainda que esta seja necessária. A base da autonomia é a proatividade, isto é, a capacidade de 'tomar a iniciativa'. Em relação ao conceito de cooperação é, portanto, a razão de ser de ter vários agentes, a comunicação é necessária para garantir a cooperação e geralmente envolve mensagens de alto nível. Por fim, para atributo de aprendizagem, eles aprendem conforme reagem e/ou interagem com o ambiente externo.

IV. A *quantidade de agentes* também é critério de classificação para os agentes. Uma diferenciação é feita entre agentes individuais e sistema multiagente. Os agentes individuais ou únicos atuam em ambientes que não contém nenhum outro agente, logo eles não são capazes de contatar outros agentes, mesmo quando estão no mesmo ambiente. Os agentes únicos contatam apenas os usuários ou informações de fontes como bancos de dados. De modo contrário, um sistema multiagente consiste em uma série de agentes que podem comunicar ou mesmo cooperar uns com os outros.

Embora os agentes de software possam ser classificados em uma outra categoria, um mesmo agente pode pertencer a vários tipos, a depender do objetivo e da ação que está realizando.

4.9.2 Sistema Multiagente

Um agente pode se comunicar, cooperar e negociar com outros agentes. Uma ideia básica é que é fácil construir um agente com pouco conhecimento especializado. Porém, na execução de tarefas mais complexas com a exigência de muito conhecimento, é necessário empregar vários agentes de software atuando em conjunto dentro de uma aplicação. Esses agentes precisam compartilhar o conhecimento, ou os resultados da aplicação podem falhar.

Nesse cenário, para VASILAKOS et. al. (2017), um sistema multiagente é uma extensão do *agente inteligente* constituído por um grupo de *agentes autônomos* os quais atuam em um ambiente para atingir um *objetivo* em *comum* ou os respectivos objetivos

individuais. Esses agentes podem *cooperar* ou *competir* uns com os outros e de certa maneira *compartilhar* ou não o conhecimento uns com os outros. Uma vez que o conceito de sistemas multiagentes é introduzido percebe-se que se procurado apresentar várias tentativas de criar metodologias para projetar e desenvolver tais sistemas. A construção de um sistema multiagente envolve não apenas características encontradas em sistemas distribuídos ou concorrentes, mas também em funcionalidades que garantam à *autonomia*, *flexibilidade* e as interações complexas com outros agentes individuais. Um exemplo é o roteamento entre redes de telecomunicações cuja informação deve trafegar de uma rede controlada por uma determinada empresa e assim seguir para outra rede controlada por outra empresa. Ambas as aplicações podem se utilizar dos recursos advindos de outras aplicações no roteamento de pacotes com mais eficiência da origem ao destino.

As razões para *agir em conjunto* está em *alocar recursos, gerenciar e/ou eliminar conflitos* sobre os interesses para alcançar as metas, pois de outra forma, essa não poderia ser realizada. Também, existe a possibilidade de melhorar a eficiência, aumentando a previsibilidade com a redução dos custos envolvidos. Em outras palavras, eles apresentam uma eficiência em sentido global da atividade.

Nesse sentido para BADICA *et.al* (2011), um sistema multiagente é desenvolvido para ser executado sobre uma infraestrutura especializada cuja finalidade é fornecer as funcionalidades necessárias para a existência da aplicação multiagente. Visto por essa perspectiva, a aplicação distribuída pode conter funcionalidades de software e de serviços para assegurar: *gerenciamento do ciclo vida do agente*, a *comunicação do agente*, a *mensagem de transporte* entre outros. Nesse sentido, fala-se em um *framework* constituído por agentes cuja infraestrutura de software dispõe dos principais artefatos de software necessários para criar o sistema multiagente.

A abordagem sistema multiagente é intuitivamente simples, pois desenvolvedores podem aproveitar a experiência em resolução de problemas encontrados no mundo real para atribuir a um agente específico. Em HAYZELDEN *et.al* (1999), tal abordagem trabalhada tendo como base o conceito de agentes fornece uma analogia apropriada para a decomposição de um problema em subproblemas e da delegação concorrentes de tarefas. Para ADELINDE *et. al.* (2009), um *sistema multiagente* é hoje considerado como uma forma interessante e conveniente de *compreender, modelar, projetar* e *implementar* diferentes *tipos de sistemas*. Eles podem ser usados como um *paradigma de programação* para desenvolver softwares. São, em particular, adequados para implantar sistemas de software distribuídos, dado o contexto computacional em que o controle global é difícil ou impossível de alcançar.

No entanto, uma questão apresentada por GATTI *et.al*. (2006) está na possibilidade de garantir a *confiabilidade*, ou seja, como ter a certeza de que o sistema vai fornecer *serviços confiáveis*, já que há gargalos críticos na disponibilidade entre os agentes. Nessa visão, a garantia quanto ao aumento da disponibilidade dos agentes se dá pela aplicação da técnica de tolerância a falhas, já que no quesito confiabilidade atribui-se mecanismos visando aumentar a interação entre os agentes.

Outro fato importante está na questão de *cooperação* em um sistema multiagente, em BUCCAFURRI *et.al*. (2001) a ideia é criar uma cooperação frutífera, com o objetivo de enriquecer o suporte às atividades dos usuários. A cooperação pode ser implementada de várias formas, a depender do conhecimento local dos agentes. O objetivo é fornecer ao usuário uma visão integrada das bases de conhecimento. Porém, a principal dificuldade é determinar quais agentes são candidatos promissores para a cooperação frutífera dado o universo de opções de agentes que operam na rede.

4.10 Modelo Dossiê

O conceito da estrutura *Dossiê* foi apresentado por SILVA (2017), a ideia parte do princípio de que qualquer transação realizada por um agente seja assinada com certificado digital. O objetivo de tal ação é garantir a identificação do agente, além de servir de subsídio gerar o indicador de reputação e de confiança no compartilhamento das fontes de informação.

A descrição do modelo Dossiê é descrito com base no cenário apresentado em SILVA (2017):

I. Um *agente provedor* p fornece um serviço a um *agente consumi*dor c. O serviço pode ser entendido como qualquer ação destinada a satisfazer as necessidades do solicitante, seja uma transação comercial, uma assistência médica ou uma mera pergunta a ser respondida.
II. Na sequência, o agente c avalia o serviço prestado e envia um *feedback* f para o agente p. O agente p armazena f localmente.
III. Os *feedbacks* recebidos e mantidos por p, são agrupados e armazenados em uma estrutura particular, denominada de *Dossiê* e denotado por $D(p)$, onde se lê "Dossiê do agente provedor p". Deve-se salientar que um Dossiê é uma estrutura que assegura a imutabilidade da informação ali armazenada.

O *conjunto de feedbacks* recebidos compõem o *testemunho* sobre o agente p, e estará disponível para consulta para qualquer agente com intenção de conferir a confiança de p. Os

feedbacks são representados por uma quíntupla $f = (c, p, i, v, t)$. Dado uma interação i, o agente c avalia o agente p atribuindo o valor v (representa um grau de confiança) para o termo t, o qual assume a dimensão *contexto*. Nesse cenário, o termo representa qualquer característica a ser avaliada como, por exemplo, em transações comerciais: preço, prazo, qualidade, atendimento, dentre qualquer outro contexto necessário para o agente.

A abordagem *Dossiê* surgiu para resolver problemas comuns nos modelos de confiança. Por exemplo, o agente não tem interesse em compartilhar experiências ou não há mensagens suficientes para identificar boas testemunhas. Para isso, o agente deve guardar localmente os *feedbacks*, com a intenção de eliminar a necessidade de que outros agentes testemunhem sobre o agente avaliado. Os dados coletados estão disponíveis localmente no *Dossiê* do agente provedor e protegido contra adulteração.

4.9.1 Criptografia aplicada no modelo *Dossiê*

Criar procedimentos visando garantir a legitimidade das informações, quando trafegadas em comunidades virtuais é uma das iniciativas abordadas no modelo Dossiê. A ideia é fornecer meios que impeçam agentes maliciosos, inseridos em uma comunidade de agentes, obter vantagens indevidas. Para coibir tal prática, SILVA (2017) usa a técnica de criptografia assimétrica aplicada nos *feedbacks* recebidos nas transações realizadas.

O modelo prever que cada agente possua o próprio certificado digital, como forma de ser reconhecido e/o identificado na comunidade de agentes. O objetivo é garantir a integridade nas mensagens trocadas e, de modo opcional o sigilo. Dessa forma, as mensagens são autenticadas por meio de certificado digital como forma de atestar a autoria das mensagens transitadas no formato eletrônico. A *Figura 26* representa a situação de envio e de recebimento de mensagens assinadas.

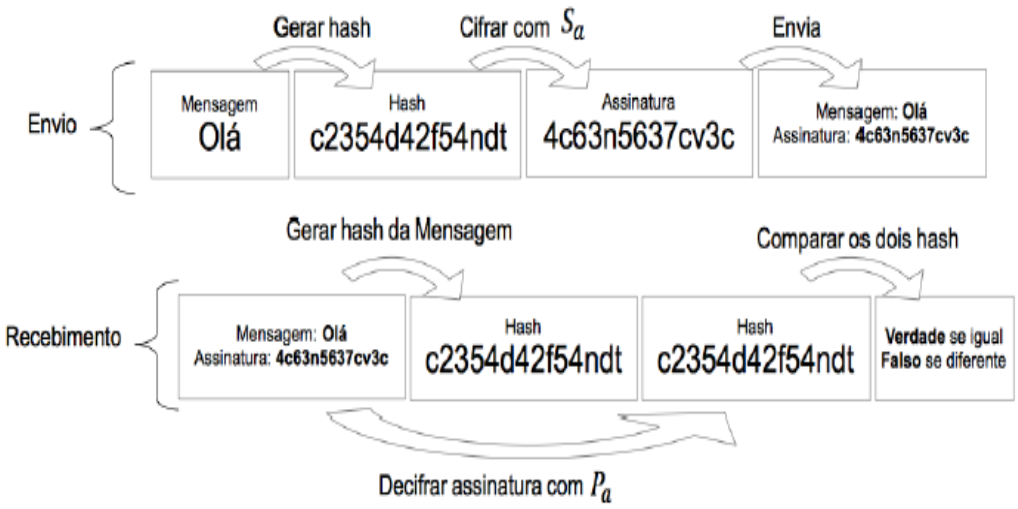

Figura 26. Verificação de mensagem por assinatura digital, SILVA (2017)

O funcionamento do processo de assinatura digital é o seguinte (cf. a *Figura 26*):

I. Um agente a possui um par de chaves: secreta Sa e pública Pa.

II. No momento em que a envia um dado Da para um destinatário, a calcula a função *hash* de Da resultando em $hDa = hash(Da)$, criptografada hDa com a chave secreta $ADa = encrypt\ (hDa, Sa)$.

III. ADa é a assinatura digital do dado Da.

IV. Em seguida, quando a enviar Da, é necessário repassar o certificado digital que contém a chave pública Sa. O destinatário da mensagem tem a atribuição de verificar se Da foi criado por a calculando novamente o *hash* da mensagem recebida hDa e, para isso decifra ADa por meio da chave pública Pa. Assim, se: $decipher\ (ADa, Pa) = hDa$ assume-se que Da foi criado pelo agente a.

4.9.2 Cadeia de blocos no *Dossiê*

O modelo *Dossiê* inova no sentido de garantir, de modo local, que os dados—*feedbacks* recebidos—estejam no *controle* do próprio indivíduo, dado que a estrutura de dados assegura a integridade das informações transacionadas por meio dos agentes. A busca está em proteger-se contra agentes maliciosos, sendo assim, a assinatura digital a garantia da imutabilidade dos *feedbacks*. Por outro lado, ainda é preciso garantir que os agentes maliciosos não façam comunicação seletiva das informações. Dito de outro modo, o modelo precisa assegurar a não retirada de informações/*feedbacks* de maneira seletiva do *Dossiê*. Como forma de resolver essa questão, SILVA (2017) usa uma estrutura de dados semelhante a uma cadeia local de

blocos liga pelo último *hash*, desta cadeia, a um *Ledger distribuído*. Essa estrutura de dados está apresentada na *Figura 27*.

O conjunto de *feedbacks*—na parte Dossiê da *Figura 27*—assume uma estrutura de árvore de *Merkle*. A raiz da árvore é resumo criptográfico do *Dossiê*. A parte das transações anteriores é conecta todas as transações recebidas pelo agente—proprietário do *Dossiê* em questão. O objetivo é poder atravessar a árvore, partindo da raiz para verificar se houve alguma mudança no *Dossiê*. Esse processo visa garantir que nenhum *feedback* inserido foi alterado, adicionado ou removido no *Dossiê*. No campo identificador do agente avaliado há um *hash* de certificado digital referente a tal agente. Com a informação deste campo é possível verificar a validade/persistência de todas as transações realizadas. Assim, em outras palavras, caso o agente—proprietário do *Dossiê*—queira eliminar um *feedback* ou iniciar uma nova estrutura de *Dossiê*, a fraude é descoberta.

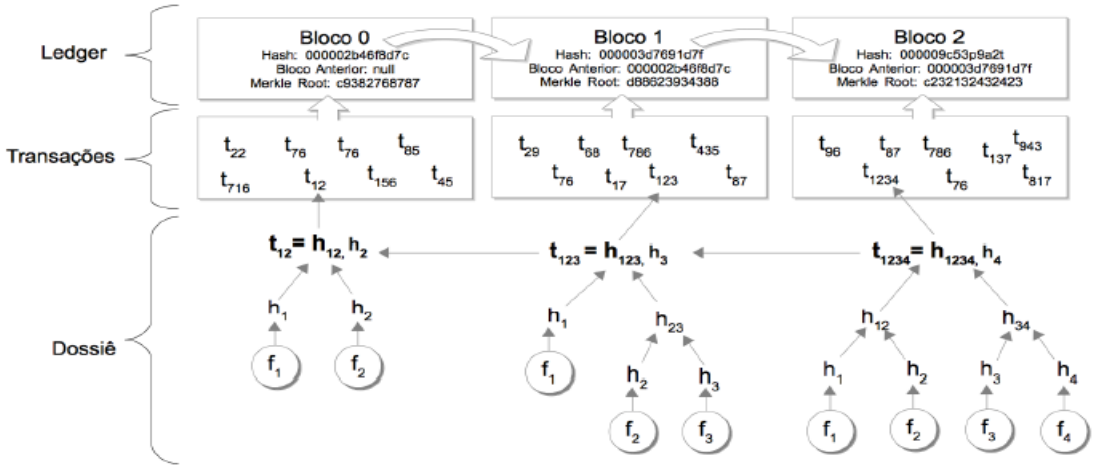

Figura 27. *Dossiê* integrado em uma estrutura de *Ledger*, SILVA (2017)

A *Figura 28* representa o percurso entre um agente consumidor ao solicitar um serviço para um agente provedor e o retorno do *feedback* do agente consumidor ao agente provedor. Nesta situação, caso o consumidor não receba a confirmação de atualização do *Ledger*, registra-se no *Ledger* uma transação de denúncia contra o provedor em questão. A denúncia ou a queixa consiste no registro do *feedback* não inserido no *Dossiê*, como também as identificações dos agentes envolvidos por tal ato. O processo de registro do *Dossiê* para ser inserido no *Ledger* inicia-se em duas fases. Com o envio do registro de *feedback* pelo agente consumidor *c*—o emissor—, e pelo agente provedor *p*—o receptor—, que tem a tarefa de enviar o certificado de registro local de *feedback* para o *Ledger* global. Após esse envio, o agente emissor fica aguardando retorno do agente receptor com o envio do *hash h* da transação para ser atestada e para identificação dentro bloco.

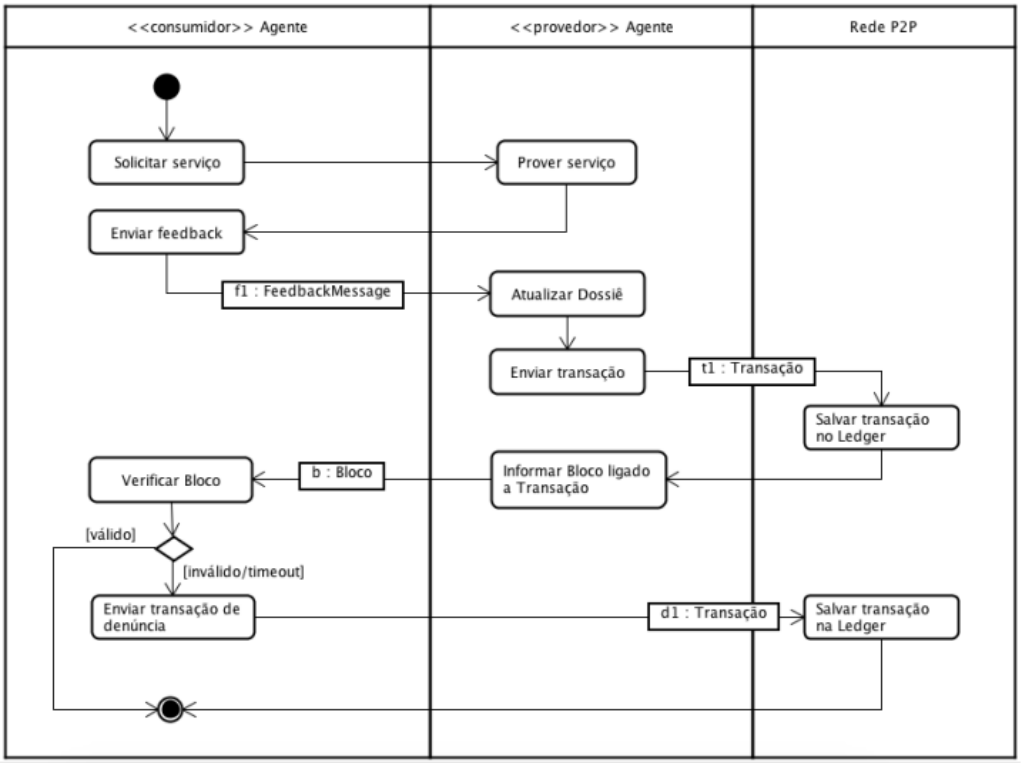

Figura 28. Envio do *feedback* e atualização do *Dossiê* no *Ledger*, SILVA (2017).

Deve-se notar que o agente consumidor aguarda uma mensagem de confirmação do registro de *feedback*. Caso tal mensagem não seja recebida, o agente consumidor registra uma denúncia no *Ledger*, incluindo no registro as partes envolvidas. Dessa forma, o método busca fortalecer a *transparência* das transações, na medida que é possível qualquer indivíduo verificar os históricos das transações entre os agentes, possibilitando, por exemplo, atribuir reputação e aferir confiança aos agentes em questão.

4.10 Modelo Trustchain

Seguindo a mesma linha de estrutura de dados cujo objetivo é fornecer métodos para colocar em prática transações seguras entre agentes em um ambiente distribuído, em OTTE (2017) *et. al.* apresentou o modelo *Trustchain* como sendo uma nova arquitetura de *blockchain*, capaz de criar transações confiáveis entre agentes sem controle central. A abordagem oferece escalabilidade, abertura e resistência à ataques Sybil, na medida que em substitui a prova de trabalho por um método próprio que estabelece a validade e a integridade das transações. Nesse sentido, essa estrutura foi construída para ser uma cadeia imutável registando as interações entre agentes.

O *Trustchain* inclui um recurso resistente a *Sybil* chamado *NetFlow*. Esse último

determina a confiabilidade de cada agente em uma comunidade *online*. O *NetFlow* garante que os agentes recebem e devolvem recursos legítimos à comunidade. Nessa proposta, mesmo que não exista o consenso global, os históricos dos registros das transações oferecem segurança e escalabilidade contínua. Nesse ponto, tem-se uma particularidade no tocante as arquiteturas *blockchain* semelhantes a arquitetura *Bitcoin* que empregam o consenso global para garantir um único *Ledger global*, pois todos os agentes operando com a *Trustchain* mantêm suas próprios redes de blocos; deve-se notar que cada bloco contém uma única transação assinada pelas partes envolvidas. Em consequência disso, tem-se a possibilidade de criação de uma solução escalável em que a taxa de transferência total da rede aumenta com o próprio tamanho da rede. No entanto, a escalabilidade acompanha o custo para garantir a consistência da cadeia distribuída de blocos.

4.10.1 Arquitetura do modelo Trustchain

O TrustChain foi construído em torno da premissa de que os agentes comunicam uns com os outros, e as transações representam objetos intercambiáveis, como por exemplo, a troca de arquivos, compra ou venda de mercadorias, transferências de dinheiro, entre outros. Cada transação é assinada criptograficamente por ambas as partes. Isso significa que a participação do usuário envolvido na transação é irrefutável. Semelhante à arquitetura *blockchain*, o *TrustChain* registra as transações em blocos e vincula/liga tais blocos usando ponteiros de *hash*. Porém, de modo contrário a arquitetura *Bitcoin*, ela não requer uma única cadeia de blocos para toda a rede, ou seja, no *TrustChain* cada agente começa com o seu próprio bloco gênese. Logo, cada agente registra as suas transações na sua própria cadeia. Cada transação no *TrustChain*, entre dois agentes, requer dois blocos. Cada bloco contém exatamente uma cópia da transação que ocorreu entre as partes. Cada novo bloco contém os seguintes campos de dados (cf. a *Figura 29)*:

- ✓ *Transação*. Esse campo registra o valor que foi trocado entre as partes. O *TrustChain* foi projetado para ser independente de aplicativo. Assim, o conteúdo de uma transação pode ser quaisquer dados serializáveis.
- ✓ *Hashes de bloco anteriores*: Os *hashes* dos blocos anteriores das cadeias de ambos os agentes se "fixam" no novo bloco. Isso é semelhante à abordagem básica da *blockchain*.
- ✓ *Chaves públicas*: A fim de identificar com exclusividade os agentes que conduzem uma transação gravam-se as chaves públicas.

- ✓ *Assinaturas*: Ambos os agentes fornecem uma assinatura digital da transação com uma chave privada possibilitando que qualquer agente possa verificar as chaves públicas dos agentes. Isso autentica a transação e prova que os verdadeiros proprietários da chave privada conduziram as transações.
- ✓ *Números de sequência*: Cada bloco da cadeia de um agente tem um número de sequência único que mostra a sua posição na cadeia de blocos.

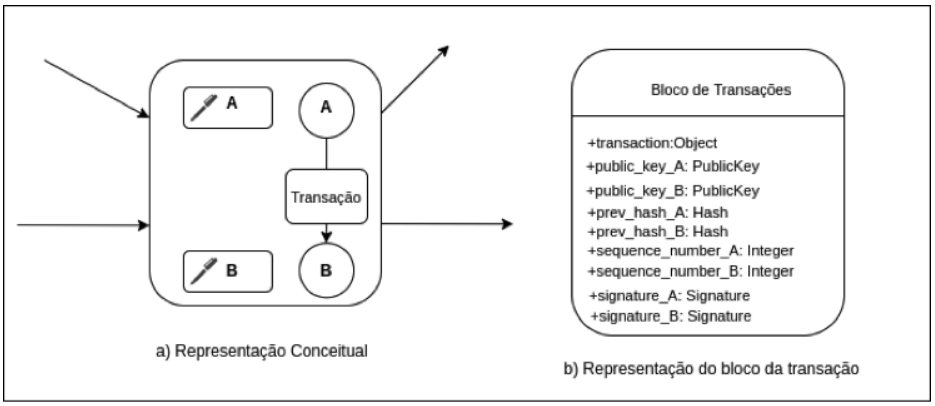

Figura 29. Representação conceitual da estrutura do *TrustChain*. HARMS (2018).

Por outro lado, na Figura 30 é apresentado uma cadeia *Trustchain* com múltiplas transações. Na parte superior mostra a cadeia de um agente *A* com *links* para vários outros blocos.

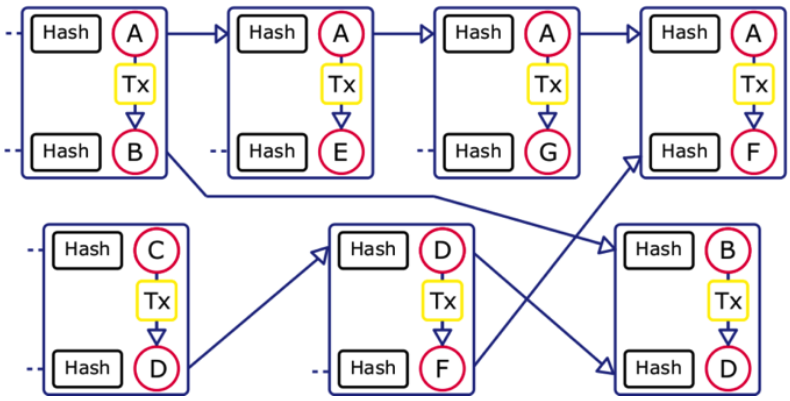

Figura 30. Modelo *TrustChain* com cadeia de blocos com múltiplas transações. HARMS (2018).

Como já dito, essa abordagem difere das arquiteturas tradicionais de *blockchain* no sentido de que cada participante mantém sua própria cadeia de transações. Arquiteturas, como por exemplo, *Bitcoin* e *Ethereum* mantêm uma cadeia única e global contendo um traço de todas as transações realizadas pelos usuários. A consistência da cadeia é garantida pelo método de consenso denominado *prova de trabalho*. Além disso, deve-se salientar que em projetos do tipo *blockchain* tradicional, pode-se impossibilitar transações múltiplas quando ocorrer um bloqueio para aumentar a taxa de transferência de transações. Por outro lado, na

abordagem do *Trustchain*, cada bloco descreve somente uma transação. Assim, após a conclusão de uma transação, ambas as partes assinam a transação e a inserem como sendo um novo bloco na cadeia de blocos de cada parte. A necessidade de que ambos os agentes assinem a transação possibilita resolver a questão em que um agente decide não anexar a transação na cadeia local, em especial, quando a transação é desfavorável a um dos participantes. Além disso, o método assegura que um único agente não reescreve a cadeia local para reordenar todas as transações, recalculando os *hashs* anteriores sem que isso exija muito esforço computacional. No entanto, caso ocorra essa ação, ela corromperá todo o histórico das transações, e ainda que se torne favorável para si, para os demais agentes tal operação ainda será falsa, na medida em que eles perceberão que os registros das transações foram alterados.

4.10.2 *Dossiê versus Trustchain*

A Tabela 7 apresenta um comparativo entre os modelos *Dossiê* e *TrustChain*:

Tabela 7. Comparativo dos atributos das estruturas de dados Dossê e Trustchain.

Atributos	Dossiê	TrustChain
Foco na comunidade de agentes	Foco no registro de *feedbacks* relativos as transações entre agentes.	Foco no registro dos *dados* relativos a transações entre agentes.
Cadeia de blocos	Cadeia local de blocos—descentralizada entre os agentes—e uso de uma referência global—*Ledger*—para o registro do último *hash* da cadeia local para garantir a integridade da cadeia local.	Cadeia local de blocos—descentralizada entre os agentes—sem referência global para garantir a integridade de cada cadeia local.
Consenso	Transação de Dossiê para registro de *hash* na referência global—*Ledger*.	Registro da transação (na cadeia de blocos de cada parte) assinada pelas partes.
Hash entre blocos	Um único *hash* entre blocos, onde o crescimento da rede se dá do último bloco do Dossiê de cada agente.	Dois *hashs por bloco, onde* cada cadeia de bloco é assinada por ambas as partes. Efetuada a transação, um novo bloco contendo-a é gerado e indexado na cadeia de blocos.
Validação de transação	Registro de *feedback* no Dossiê da parte contratada e último *hash* no *Ledger* global usando um método seguro .	Registro da transação—na cadeia local de bloco de cada agente—assinada por ambas as partes usando um método seguro.
Segurança de dados	Garantida por meio de consenso global do *Ledger* e denúncia de alteração na cadeia de blocos.	Garantida por meio de consenso local e denúncia de alteração na cadeia de blocos.
Testemunho	Requer o registro do *hash* da última transação do agente no *Ledger* global para dar como válido o conteúdo do *Dossiê* de cada agente.	Requer testemunho das partes sobre a validade das cadeias de blocos, e denúncia de alteração na cadeia de blocos.

Além disso, é preciso reforçar, com base no exposto na *Tabela 7* e na *Figura 30*, que o modelo

TrustChain pode englobar muitos cenários para toda a cadeia de blocos. Nesse sentido há diversos registros imutáveis que se formam com base nas ramificações das transações dos agentes. Essas ramificações são formadas por meio de ligações duplas entre os blocos, onde cada ligação é responsável por alinhar as transações de um agente em particular. Porém, a outra parte tem a responsabilidade de montar uma cadeia de transações ligando-se com os outros agentes com que o agente negociou. Nesse ponto, caso ocorra alteração indevida em um bloco, os demais agentes vão perceber a alteração, pois a percepção se dá pela quebra de igualdade da estrutura ligação com a estrutura dos demais agentes da cadeia de blocos. Esse cenário configura um tipo de denúncia de quebra de estrutura aos demais agentes que participam da ramificação.

4.11 Considerações do Capítulo

Inicialmente, nesse *Capítulo* foram apresentados os modelos de *identidade digitais*, colocando em valor as questões de privacidade dos dados pessoais em especial dentro do modelo de *identidade digital Auto Soberana*. Tal modelo é defendido nesse trabalho como instrumento necessário para dar ao usuário controle sobre os seus próprios dados. Para isso, foi necessário examinar as arquiteturas e conceitos com vistas as aplicações distribuídas, no uso, por exemplo da tecnologia *blockchain*. Em seguida, foram abordadas questões sobre agente de software focando apenas nas suas principais características, finalmente, dentro desse cenário, foram abordadas as estruturas de dados de seguras *Dossiê* e *Trustchain* como subsídio para fundamentar a abordagem que permite o registro do local de dados e identidade digital, favorecendo uma arquitetura distribuída e centrada no usuário.

5 Identidade do agente assegurada pelo modelo *Auto Soberano*

5.1 Introdução

Esse capítulo visa examinar aplicação de um *modelo de identidade digital* que permita ao usuário o *controle sobre as próprias informações*, quando este atua em um ambiente descentralizado. A fundamentação desta iniciativa encerra o modelo *Identidade Digital Auto Soberana* (*Capítulo 3 e Capítulo 4*), aplicada no contexto de um *sistema de agentes,* tomando como arquitetura básica o *modelo Dossiê* (SILVA, 2017), criado no *laboratório de Agentes de Software* do PPGIa/PUCPR. A ideia é que o *Dossiê* atue em conjunto com o *modelo de identidade digital Auto Soberana* em cenários em que o indivíduo compartilha informações com o mundo externo. Nesse cenário, os indivíduos são representados agentes—ou mais especificamente agentes de software—, que podem denotar virtualmente agentes seres humanos. Esses agentes podem assumir basicamente dinamicamente dois papeis, em função de quem toma a iniciativa de iniciar uma transação/interação, doravante nomeados de consumidor/cliente—quem inicia uma transação/interação—, agente provedor/servidor—quem se envolve em uma transação já inicializada.

O modelo *Dossiê* permite qualquer indivíduo, por meio da rede de agentes, compartilhar informações—*feedbacks*—sobre si. No entanto, o compartilhamento requer da autorização/desejo do agente proprietário das informações.

MUKTA *et. al.* (2020) enfatiza que o compartilhamento dos dados é uma divulgação seletiva e isso ocorre quando uma credencial genérica é emitida com apenas os atributos necessários para serem revelados pelo *agente verificador*. O *agente verificador* só vê o atributo divulgado para aquele contexto da transação. De modo semelhante, na estrutura *Dossiê* a seletividade das informações ocorre em função de qual tipo de informação que se deseja verificar para o histórico dos serviços prestados do agente no contexto em análise. Deve-se notar que na versão original do *Dossiê* não se previa a divulgação parcial do conteúdo do *Dossiê* de cada agente.

Embora, o grau de confiança entre os agentes possa variar de uma interação para outra, a necessidade de validar as identidades de modo seguro e preservar a privacidade é universal. Aqui, assume-se a necessidade de que os indivíduos e/ou entidades possam criar e/ou

gerenciar as próprias formas de identificar-se de forma descentralizada e *sem depender* de um provedor *terceirizado de informação* para validar as informações originadas dos agentes.

Por isso, ao contrário das soluções existentes, onde muitas delas estão estruturadas na *perspectiva da organização*, o modelo *de identidade Auto Soberana* se estrutura para funcionar da *perspectiva do indivíduo*, assumindo dessa forma o *papel de sujeito* ao determinar a forma e como vai identificar-se. Na arquitetura dos *modelos de identidades digitais* mais comuns encontrados na literatura e aceitos pelas organizações, tem-se que a grande maioria ou são *centralizados no próprio provedor de serviços* ou, de outro modo, aceita-se que a *validação das credenciais* dos usuários ocorra por meio de uma *terceira parte confiável*, característica essa muito comum do *modelo de identidade digital Federado*.

Em geral, nos modelos apresentados, os usuários não têm o controle e nem a posse dos seus próprios dados. De modo conceitual, o *propósito da identidade digital* é de ser o instrumento responsável pelo *cuidado dos dados pessoais*, criando-se procedimentos para garantir a *validação dos dados* no contexto de uma aplicação que permite realizar as *transações digitais*. No entanto, um aspecto crítico de qualquer esquema de *identidade digital* é como *proteger os dados* e garantir a *privacidade do indivíduo*. Nesse sentido, o *controle* e a *gestão dos dados* deveriam ficar *a cargo do indivíduo* quando houver interação com outros agentes.

De certa forma, buscou-se entender, a partir das propostas apresentadas na literatura, os caminhos para assegurar a *imutabilidade de dados sensíveis*, tanto no momento do *compartilhamento proativo de informações pessoais*, como também do *histórico de atividades* e *serviços* que o usuário queira compartilhar.

5.2 Gestão local dos dados

Assumindo que indivíduo atua dentro do modelo de identidade digital *Auto Soberana*, e que esse modelo tem pontos em comum com o modelo *Dossiê*, a *condição necessária e suficiente* para que a *gestão local e segura de dados* possa ocorrer é que o *indivíduo* tenha a *posse* e o *controle* sobre os próprios *dados*. Nesse cenário, o usuário—representado por *agente software*—pode comunicar/interagir com outros agentes para atender necessidades próprias. A comunicação permite que os agentes coordenem ações e comportamentos, resultando em ações consistentes para que eles possam alcançar estados considerados desejáveis ou indesejáveis. Como os recursos são limitados, os agentes devem ser capazes de coordenar as suas atividades para alcançar metas globais.

Deve-se assegurar uma estrutura mínima necessária para garantir que os dados compartilhados não sejam alterados durante o percurso. Exige-se, então, que o *Dossiê* de cada agente esteja assentado sobre uma plataforma que garanta a imutabilidade dos registros, nesse caso adotando-se a tecnologia *blockchain*.

Responsabilidades podem ser atribuídas aos agentes, e eles podem trabalhar de forma coordenada em prol de um objetivo em comum ou compartilhado. Em termos de distribuição, cada agente é um nó, com características intrínsecas, pelas quais tem o controle local sobre os seus dados. Porém, em geral, só há sentido em um sistema transacional, que cada agente que se relaciona com outro agente, exista um meio formal de atribuição de responsabilidades, por exemplo, por meio de instrumentos do tipo *contrato*, em que as partes se colocam em acordo sobre um termo.

A relação estabelecida entre os agentes envolve um processo que visa atender os interesses das partes envolvidas em relação a um termo, que pode ser relativo a um produto ou um serviço. Neste processo, cada envolvido possui um único papel dentro do conjunto de papeis definidos (e.g., papel de consumidor, de provedor de serviço). A relação pode envolver, por exemplo, a utilização de métodos que coloque em prática a realização das atividades necessárias para um compartilhamento *proativo* ou *estimulado* de dados, representando os demais atores envolvidos (e.g., agentes atuando em rede simulando uma estrutura de Marketplace). Neste caso, o objeto transacionado é o próprio dado.

5.3 Privacidade dos dados baseadas em cadeias de bloco híbridas

O interesse aqui porta sobre o modelo de agente que tem o controle sobre a sua identidade digital—denominado *modelo Auto Soberana*—, bem como o controle sobre o seu próprio *Dossiê*. A *Figura 31* representa o processo de atualização de dados no *Dossiê*. A premissa é de que a imutabilidade e a privacidade dos dados de cada agente são asseguradas pela estrutura *Dossiê*, baseada em cadeias de blocos híbridas.

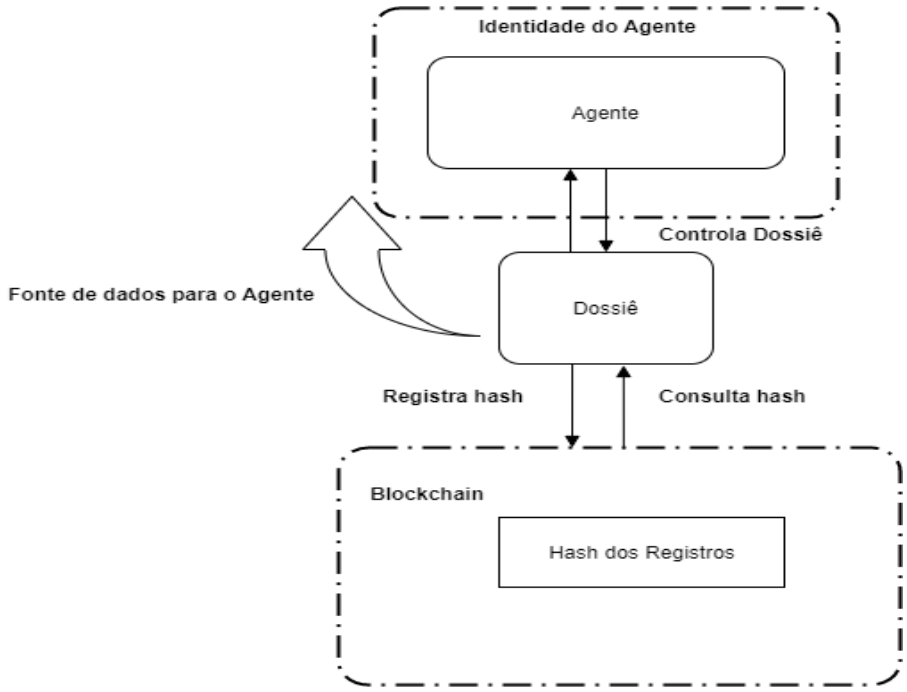

Figura 31. Controle do *Dossiê* pelo agente e atualização na rede *blockchain.*

Para garantir a imutabilidade dos dados no *Dossiê* tem-se que:

A. Os dados são locais assinados por chave *hash*, e a última chave é registrada em uma rede *blockchain*;
B. Os dados são fornecidos por meio de assinatura ou de serviço *push;*
C. O agente é o proprietário dos dados e sobre eles tem o controle e a outorga para realizar o compartilhamento *proativo* com qualquer outro agente;
D. O caminho da atualização do dado é o próprio *Dossiê*;
E. A tecnologia *blockchain* garante a imutabilidade dos dados, a arquitetura pode ser pública ou privada, com o consenso comum ou não, pois a decisão de qual arquitetura utilizar depende do tipo de agente. O agente pode representar a virtualização dos interesses de uma pessoa. Ele também pode ser estendido para a virtualização de uma empresa ou órgão do Governo. No entanto, o caminho que liga um agente ao outro é realizado por meio de *smart contract;*
F. A localidade dos dados e do controle no usuário—ou seu representante virtual—, decide sobre o armazenamento por sua conta e risco. Em outras palavras, o agente tem a posse e o controle sobre os dados, porque os dados estão disponíveis em um repositório que o usuário acredita ser seguro;
G. Os dados dos usuários estão armazenados no *Dossiê* e na rede *blockchain* fica armazenado o último *hash* da cadeia de blocos do *Dossiê*, conforme mostra a *Figura*

32, representando o processo de atualização dos dados no *Dossiê* e o correspondente *hash* da cadeia de blocos. Caso algum agente queira verificar se os dados do *Dossiê* são *fidedignos*, ele pode fazer verificando o último *hash* para aferir a *autenticidade* dos demais blocos.

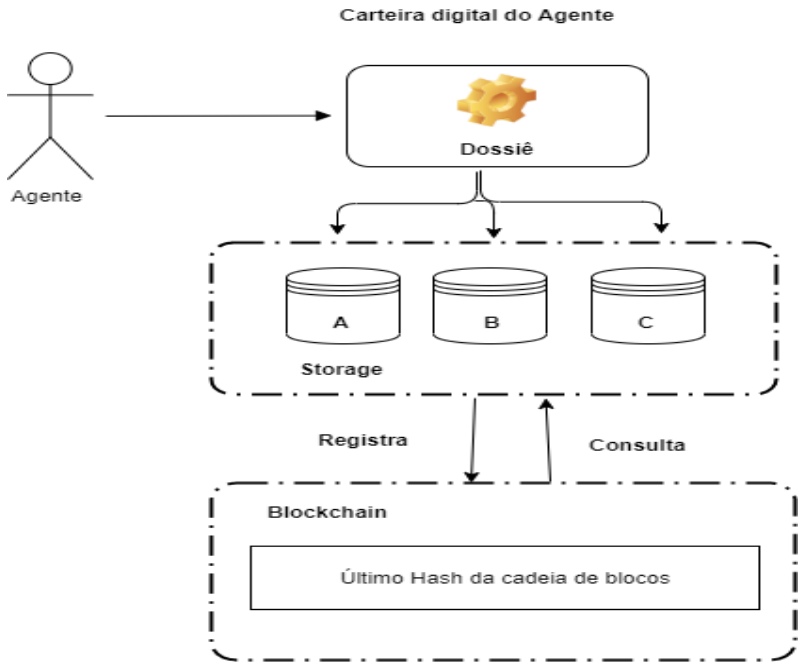

Figura 32. Atualização dos dados na *carteira digital* do agente e último *hash* atualizado na *blockchain*.

5.4 Modelo *Dossiê* em conjunto com a *identidade digital*

Como já dito, parte do objetivo desse trabalho é utilizar a estrutura *Dossiê* proposto por SILVA (2017), como modelo de compartilhamento dos dados controlados pelo usuário em conjunto com a estrutura do modelo de Identidade Digital *Auto Soberana*, ambas estruturas baseadas na arquitetura *blockchain*. Sobre o modelo *Dossiê* foi acrescentada uma *camada* para comportar a identidade digital do agente (cf. a *Figura 33*).

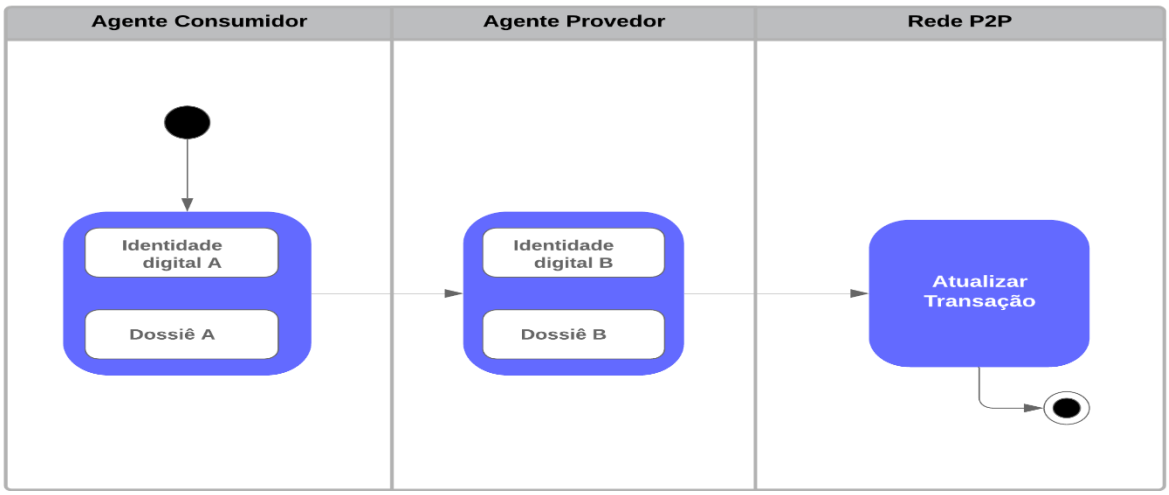

Figura 33. Modelo de identidade *Auto Soberana* aplicado na estrutura *Dossiê*.

Ilustração: o *agente consumidor c* tem a identidade digital *A* e quando *c* interage com o agente provedor *p* ocorre a verificação da identidade de ambos os agentes, *p* pode oferecer um serviço *s* para *c* e nesse momento *c* pode atestar o quão confiável é *p* verificando as informações relativas aos *feedbacks* presentes no *Dossiê* de *p.* A transação é finalizada com a atualização dos históricos na rede *blockchain*.

A identidade dos agentes comporta qualquer informação que represente o agente. As informações podem ser categorizadas nas principais dimensões que represente o agente: *quem eu sou? o que eu faço? de onde vim?* Ou naquilo que o agente possui: *O que eu tenho? Carros, imóveis, dinheiro, ativos financeiros.* Os agentes têm o *direito de outorga* sobre os dados. Por exemplo, se um agente *provedor* possui bens do tipo veículo ou imóvel, então quando realizar uma transação com um outro agente *consumidor*, o agente *provedor* pode avaliar se a informação sobre seus bens para aquela transação é necessária; a exemplo do que ocorre quando um cliente solicita um empréstimo para uma instituição financeira.

5.5 Dossiê local como forma *fidedigna* de dados

O *Dossiê local* sendo uma estrutura de dados, representa de forma *fidedigna* e *autêntica* o *histórico de vida* do seu proprietário. O modelo permite que cada agente guarde o *histórico de transações, incluindo feedbacks* e para *assegurar que os dados sejam imutáveis* parte da informação sejam registrados em uma cadeia de blocos pública: um *Ledger*.

Nessa abordagem, enfatiza-se que no *Ledger* são guardadas apenas as *referências das identidades digitais* com quem se interagiu em vida. Nesse caso, a estrutura das *identidades digitais* se comporta como uma *aplicação orientada a serviços.*

5.5.1 Gerenciamento de chaves descentralizadas

O *Dossiê* representa a entidade que possui uma chave mestra para gerenciar outras sub-chaves, as quais são utilizadas para assinar transações para contas de identidades diferentes. Pode-se operar também sobre uma arquitetura descentralizada (DPKI) para a geração de chaves (cf. a *Figura 35*). Essa arquitetura é uma evolução em relação a estrutura tradicional de PKI baseada em uma Autoridade Certificadora (CA) [AHMED et. al. (2020)]. O objetivo da DPKI é *evitar a dependência de terceiros*, ou seja, o uso da arquitetura descentralizada para garantir segurança e *integridade do dado* quando adicionado à cadeia de blocos. Na *Figura 34* é representado o fluxo para a geração do certificado para um *agente*, seguindo a arquitetura *CA*.

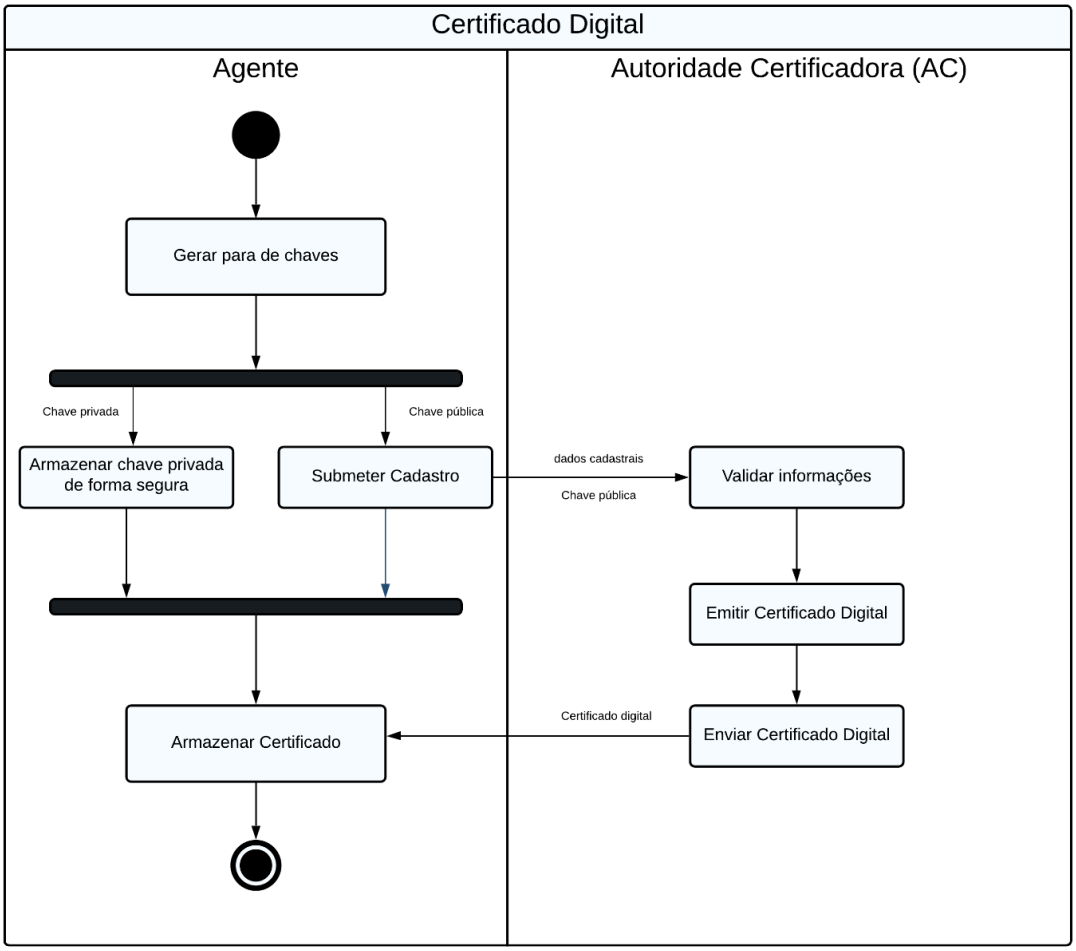

Figura 34. Identificação do agente por meio de *certificado digital*. Adaptado de SILVA (2017).

No entanto, ao considerar o cenário onde a estrutura *Dossiê* atua em conjunto com o modelo de *identidade digital Auto Soberana*, a geração dos pares de *chaves deve ser descentralizada*, isto é, não são geradas por uma *entidade centralizadora*, mas a partir do usuário dono da informação. A *Figura 35* representa o fluxo da geração dos pares de chaves

no modelo *descentralizado do ponto de vista do usuário*.

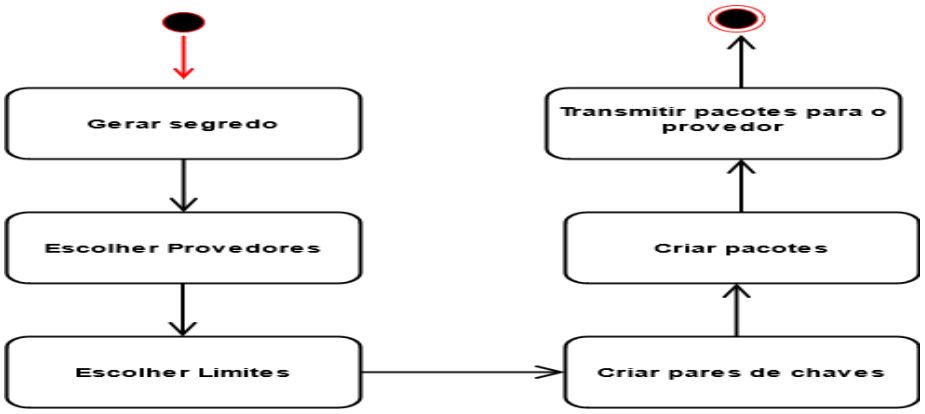

Figura 35. Geração descentralizada de chaves de *Dossiê* em conjunto com o modelo de identidade digital *Auto Soberana*. SOLTANI et. al. (2020).

Para SOLTANI *et. al.* (2020), os *protocolos* necessários para suportar a arquitetura de *chaves descentralizadas* devem:

I. *Garantir* o registro de serviços e geração de chaves (cf. a *Figura 39*);
II. *Assegurar* que ocorra o *backup* das chaves; e
III. *Permitir* que as chaves possam ser recuperadas em caso de perda/esquecimento.

A etapa de verificação é usada para permitir que os agentes envolvidos tenham a garantia da veracidade da identidade antes de se envolverem na troca ou no consumo de serviços.

5.5.2 Armazenamento dentro (*On*) e fora da cadeia (*Off*) do *Ledger*

As *aplicações descentralizadas* (DApps) representam uma solução que permite o agente/usuário ter o *controle/posse* sobre os seus próprios dados. Para ALBOAIE *et. al.* (2020), além dos *custos de desenvolvimento* de aplicações DApps, há questões de como lidar com *informações privadas* visto que os processos de *consenso* e validação são pressionados para manter a maior parte dos dados públicos. Nesse ponto, há obstáculos de uso, em especial quando há *informações do tipo privada* a exemplo de *segredos comerciais*. Dessa forma, não importa o *anonimato* ou as *estratégias de criptografia* quando os dados armazenados estão na rede *blockchain*, já que existe a possibilidade de correlacionar os dados notariados dentro do *Ledger* com dados externos; isso de certa forma é indesejável e representa um obstáculo para a adoção generalizada de DApps.

No entanto, uma solução apresentada em ALBOAIE *et. al.* (2020), LIU *et. al.* (2020)

e ABID *et. al.* (2021) considera o uso de armazenamento de dados *dentro* (*On*) e *fora* da *cadeia* (*Off)* os dados no *Ledger*:

I. *Dentro da Cadeia (On).* Utiliza a *blockchain com permissão privada ou pública* para assegurar as *verificação das chaves criptográficas* e servir como *registro de dados verificável à prova de violação*.

II. *Fora da Cadeia (Off).* Utiliza o armazenamento IPFS (*InterPlanetary File System*[8]) ou EDPS (*Encrypted Distributed File System*)[9] para persistir os dados sensíveis do usuário ou da entidade. Nessa proposta apenas o *hash IPFS* ou *EDFS* é armazenado na cadeia *On*, possibilitando que informações *confidenciais* nunca sejam reveladas a outras pessoas na rede *blockchain.*

A *Figura 36* representa uma proposta de uso da arquitetura de *armazenamento dos dados On/Off* aplicado no modelo *Dossiê*.

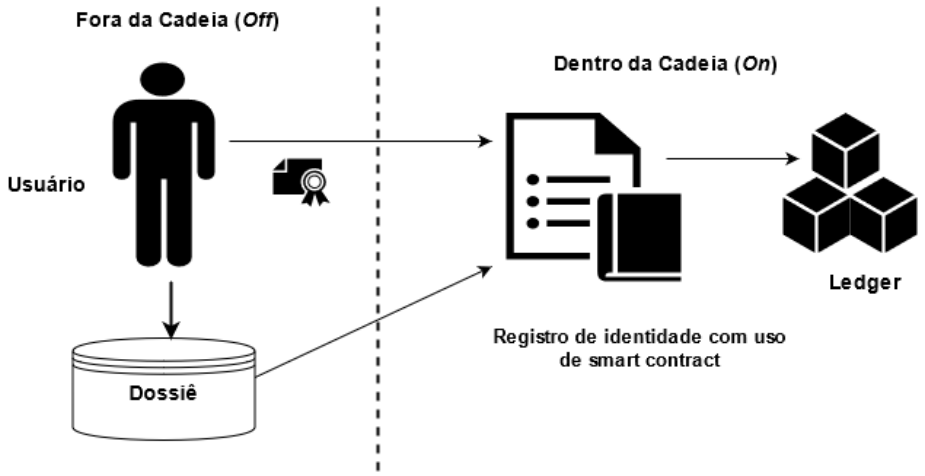

Figura 36. Arquitetura de armazenamento dentro(*On*) e fora(*Off*) aplicado no modelo *Dossiê*.

As informações provenientes do *Dossiê* são armazenadas usando *hash IPFS* ou *EDFS* na estrutura *fora da cadeia*. E na rede *blockchain* permanece apenas as referências dos *hashes* dos dados originados do armazenamento de *fora da cadeia*

5.5.3 Seletividade de dados

A seletividade de dados presente no modelo *de identidade digital Auto Soberana* permite as

[8] https://ipfs.io/
[9] https://evannetwork.github.io/

partes decidirem quais atributos da identidade estarão contidos na credencial. Em MUKTA *et. al.* (2020), uma vez emitida a credencial, há a necessidade de satisfazer requisitos específicos do *verificador de destino da identidade* do titular, sem no entanto revelar dados extras. A *aplicação do requisito de seletividade de dados* aplicados no modelo Dossiê é ilustrado na *Figura 37.*

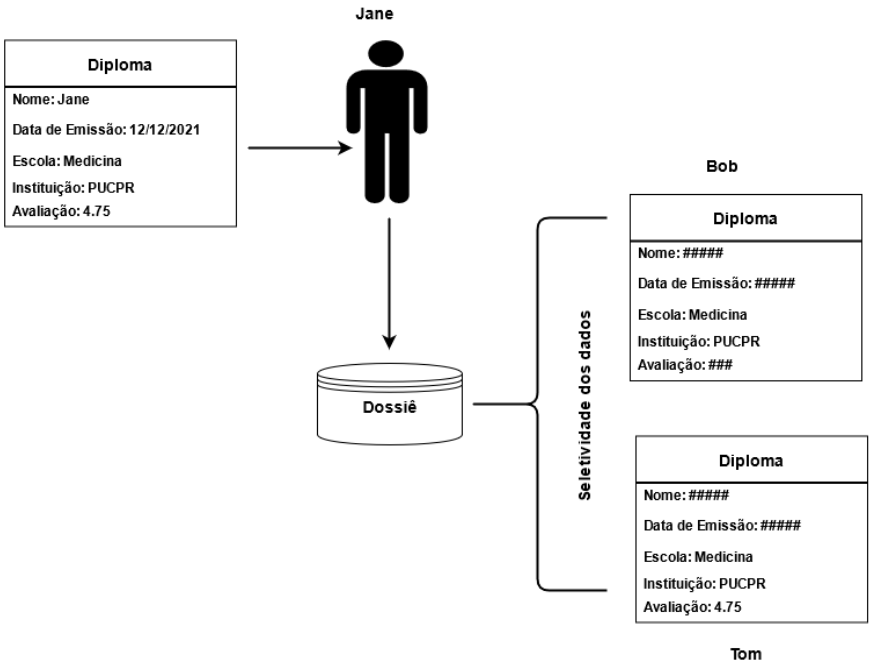

Figura 37. Seletividade dos dados aplicado no modelo *Dossiê.*

O *Dossiê* de cada agente é uma fonte de dados. No entanto, ao trazer o requisito de *seletividade de dados* nós nos apropriamos do conceito do modelo Dossiê, mas não de forma total, pois originalmente a estrutura *Dossiê*, em relação aos históricos dos *feedbacks* foi planejada para que as informações sejam mostradas de forma integral quando do compartilhamento delas entre agentes. Outra questão importante é que se estende o conceito de *feedbacks* para a ideia de um conjunto de listas encadeadas dentro de uma árvore de *Merkle.* Nessa abordagem, a lista contém qualquer informação que faça sentido para o sujeito. Nessa perspectiva, portanto, entende-se que é possível acessar apenas parte do *Dossiê* de cada agente, seguindo o princípio da minimização da exposição da informação. Os dados presentes no Dossiê estão criptografados e a visualização deles se dá pelo compartilhamento de chaves específicas que habilitam acessar parte destes dados. Por exemplo, digamos que a transação da *Figura 41*, entre *Bob* e *Tom*, um dos agentes queira se certificar das notas informadas. Para isso, deve-se assegurar, em primeiro lugar, se informação é verdadeira e, em seguida, apresentar algum método que possibilite que seja visualizada apenas a informação

desejada/acordada. Nesse cenário, a primeira parte—que a informação verdadeira—é verificada com base no último *hash* inserido na cadeia de blocos do *Ledger* global, já a visibilidade parcial da informação ocorre por meio de uma chave compartilhada entre as partes para o fim requerido. Nesse sentido, a seletividade da informação dentro do modelo *Dossiê* requer:

I. criptografar a informação para a sua proteção.
II. permitir a visualização parcial dos registros de dados/informações
III. registrar as informações de propriedade de cada agente em uma sua cadeia local de blocos.
IV. registrar último *hash* da cadeia local de cada agente no *Ledger global* para garantir a integridade de cada *Dossiê* local.
V. manter—*by default*—toda informação de cada agente como não visível as outras partes.
VI. enviar, ao agente parceiro, uma chave para a visualização apenas da informação de interesse.

5.5.4 Conformidade com as Leis de Proteção dos Dados

Na Tabela 6—no *Capítulo 4*—, foi apresentado um *comparativo* entre as *leis de proteção de dados*, em especial a *GDPR* e a *LGPD* considerando o *contexto de aplicação* baseada no modelo de identidade digital *Auto Soberano*. No entanto, ao considerar a atuação em conjunto com o modelo *Dossiê*, entende-se que há *conformidade* de atendimento aos *requisitos legais* das leis de proteção de dados, em especial em relação a *minimização de dados* e do *consentimento* presentes no *art. 6 e 18* da Lei nº 13.709 / 2018. O armazenamento *dentro* e *fora* da cadeia do *Ledger* favorece manter os dados sensíveis com o proprietário do dado, pois apenas os *hashes* gerados no formato IPFS ou EDFS atuam como *indicadores de controle* sobre os dados sensíveis e permitem também que seja realizada a *Accountability*, ou seja, a prestação de contas para o "dono" dos dados.

5.6 Resumo dos Trabalhos

Para realização desse trabalho foram selecionados artigos representativos da área de estudo, em especial, aqueles que abordam o modelo de identidades digitais *Auto Soberana* no contexto de aplicações distribuídas. Além disso, centrou-se esforços em trabalhos da área de agentes software, em particular, nos modelos que permitem a gestão local de dados, a exemplo

do modelo *Dossiê*. A *Tabela* 8 apresenta alguns dos trabalhos examinados, bem como, a apresentação da nossa arquitetura, a qual se encontra em destaque na última linha desta mesma tabela.

Tabela 8. Quadro de trabalhos relacionados.

Trabalho	Proposta	Resultado
SILVA (2017)	Modelo de confiança, denominado *Dossiê*, que agrega fontes de informação para avaliar o comportamento de um agente.	Maior eficiência na escolha de agentes parceiros.
SHETTY *et. al.*(2018)	Governança em sistemas de saúde.	Registros médicos com arquitetura desenvolvida para preservar a privacidade do usuário.
STOKKINK et. al. (2018)	Identidade digital baseada em *blockchain* legalmente válida em nível de passaporte.	Modelo de reivindicação para atestar identidades Auto Soberanas com *status* legalmente válido.
HARM (2018)	*Ledger* para registrar a troca de informações entre agentes confiáveis.	Experimento e implementação de ferramentas em código aberto.
STEVENS (2018)	Método de identidade digital *Auto Soberana* em programas de transferência de renda.	Gerenciamento de identidades digitais centralizada no usuário.
GEBRESILASSIE *et. al.* (2020)	Gerenciamento de identidade de dispositivos IoT com base na identidade *Auto Soberana*.	Identidade de dispositivo e gerenciada com segurança durante todo o seu ciclo de vida.
AHMED *et. al.* (2020)	Estrutura para identificar chamadas fraudulentas de serviços bancários e evitar possível perda de contas pessoais.	Modelo *Auto Soberano* fortalece o processo de conhecer o cliente, aumentando a confiança de agências terceirizadas em serviços financeiros.
BOUWENS (2020)	Modelo de identidade digital *Auto Soberana* em programas de transferência de renda por meio de aplicações mobile.	Suporte na implementação de sistema de identidade digital *Auto Soberana*.
ALBOAIE *et. al.* (2020)	Abordagem para a privacidade e controle de dados na construção de cadeias de blocos.	Garantia de propriedade de dados e controle de dados adequado para pessoas e empresas.
HOUTAN *et. al.* (2020)	Coleta de dados médicos, especialistas e prestadores de serviços de saúde no atendimento ao paciente.	Uso de identidade diigital *Auto Soberana* no gerenciamento dados e identidade do paciente.
HASAN *et. al.* (2020)	*Blockchain* com identidade *Auto Soberana*, *proxies* de criptografia e armazenamento descentralizado, e sistemas de arquivos IPFS.	Passaporte médico digital e certificado de imunidade para teste da COVID-19.
LIU *et. al*. (2020)	Modelo de arquitetura em *Ledger*.	Persistência de dados em camadas de serviços.
BANDARA *et. al.* (2021)	Carteira digital para manter identidades digitais em conjunto com os dados de locomoção do usuário.	Informações de rastreamento digital para enfrentamento da COVID-19.
ABID *et. al*. (2021)	Registro de certificado de saúde digital.	Preservação da privacidade baseada em *blockchain* para emissão e verificação de certificado de teste/vacina COVID-19.
Nossa Proposta	Dossiê como fonte de informação para gerir a identidade digital de um conjunto de agentes quando atuam em rede.	Compartilhamento de dados com base no modelo de identidade digital *Auto Soberano*, tendo como fonte de dados única de informação o *Dossiê* de cada agente.

6 APLICAÇÃO

A realização desse trabalho segue a premissa de que o modelo denominado *identidade digital Auto Soberana* atua em conjunto com o modelo *Dossiê*. O *Dossiê* é a fonte de informação mantida por cada agente, em uma abordagem descentralizada de dados e de controle. Com base no exposto e já apresentado nos capítulos anteriores, o resultado desse estudo é mostrado por meio de um protótipo, uma interface construída em ambiente *WEB*, que embora executado em servidor local, permite ilustrar o conceito de identidade digital *Auto Soberana*, atuando em conjunto com o esquema *Dossiê*.

6.1 Cenário

O cenário visa simular a interação entre agentes *consumidores* e *provedores de serviços*, em um ambiente de troca denominado *Marketplace*. Cada agente detém o seu próprio *Dossiê*, como fonte de dados *fidedigna* e *imutável* que serve de base para o cálculo da confiança e da reputação, como também serve de fonte para subsidiar a criação e verificação da identidade *Auto Soberana* de cada agente. Para essa situação, apresentaremos um ambiente de simulação de *contratação de serviços* de natureza distintas a partir de um contexto. O *contexto* representa aquilo que o agente está realizando naquele momento, podendo ser uma *compra* ou *venda de serviços*. A ideia desse simulador, não é a de realizar investidas como a de um pregão eletrônico, mas de apresentar um ambiente que permita a um agente consumidor escolher outro agente provedor como base nos *feedbacks* recebidos e armazenados na estrutura *Dossiê* do agente provedor, e ainda verificar a identidade desse agente. Em relação a identidade do agente, ela é criada *em função do contexto* onde o agente está inserido. A exemplo, se o *agente* é um *comprador de um serviço*, a identidade criada é com base nas informações deste contexto. Em outras palavras, se a aplicação é relativa a uma compra de um veículo entre agentes vendedor e comprador, as informações necessárias possivelmente se limita ao histórico de venda do agente vendedor e ao histórico de compra do comprador. Diferentemente, se os agentes estão inseridos no contexto onde uma das partes é um órgão do Governo, para tal contexto a composição da identidade dos agentes assumem características distintas, já que a quantidade de informação necessária para decidir se contrata serviços não

está no mesmo escopo de abrangência quando a outra parte é um órgão oficial ou autoridade a qual precisa se reportar; é o que acontece na cobrança de impostos por parte da Receita Federal já que a quantidade de informações a serem mostradas deve ser suficientemente para isentar ou comprovar o valor do tributo cobrado.

6.1.2 Descrição do simulador

No ambiente simulado de *Marketplace* há agentes entre si, buscando parceiros por meio de estratégias vencedoras. Nesse cenário, o simulador apresenta as seguintes regras:

1. Ao iniciar, no tempo t_0 tem-se *dois agentes*, um do tipo *consumidor* e outro *provedor de serviços*. Cada um deles com o seu próprio Dossiê e como não há ainda interação entre agentes não há ainda nenhum *feedback* registrado, logo não há elementos suficientes para compor o cálculo da confiança e nem da reputação. No entanto, mesmo no momento t_0 a identidade do agente já existe. Nesse caso é uma identidade incipiente originada do nascimento do próprio agente.
2. No tempo t_1, o simulador segue de modo finito, possibilitando que todos os agentes interaja um com os outros.
3. Quando um agente consumidor seleciona um agente provedor de serviços é estabelecido um contrato entre eles, por meio da composição do protocolo de intenções para o consumo do serviço.
4. Após a realização do serviço contratado, o agente consumidor envia um *feedback* de valorização positiva ou negativa da realização do serviço. Nesse momento, o *Dossiê* do agente provedor é atualizado.
5. O agente avaliado pode se servir dos dados do *Dossiê* para compor a identidade digital *Auto Soberana* baseada no contexto de consumo de serviços, já que no *Dossiê* há históricos das atividades nas quais o agente participou e essas informações subsidiam os atributos necessários para compor a identidade do agente.
6. Os agentes podem solicitar ou fornecer *feedbacks* na prestação ou no consumo de serviços para outros agentes.
7. Um agente malicioso podem atribuir um valor negativo a um agente, mesmo sendo este um agente honesto.
8. O agente prejudicado para defender-se pode utilizar-se do próprio histórico de transações para comprovar a sua reputação; nesse caso parar validar a confiança

requer uma decisão/interação dos demais agentes envolvidos.

9. A identidade do agente é formada baseada em informações originadas no contexto, por exemplo, uma compra de imóvel, de veículos ou a prestação de informação a Receita Federal.

A seguir na Figura 38, representa o momento t_0 e t_1 da *criação do Dossiê* e da *interação* entre o *agente provedor* e *consumidor*, com a respectiva atualização do *Ledger*.

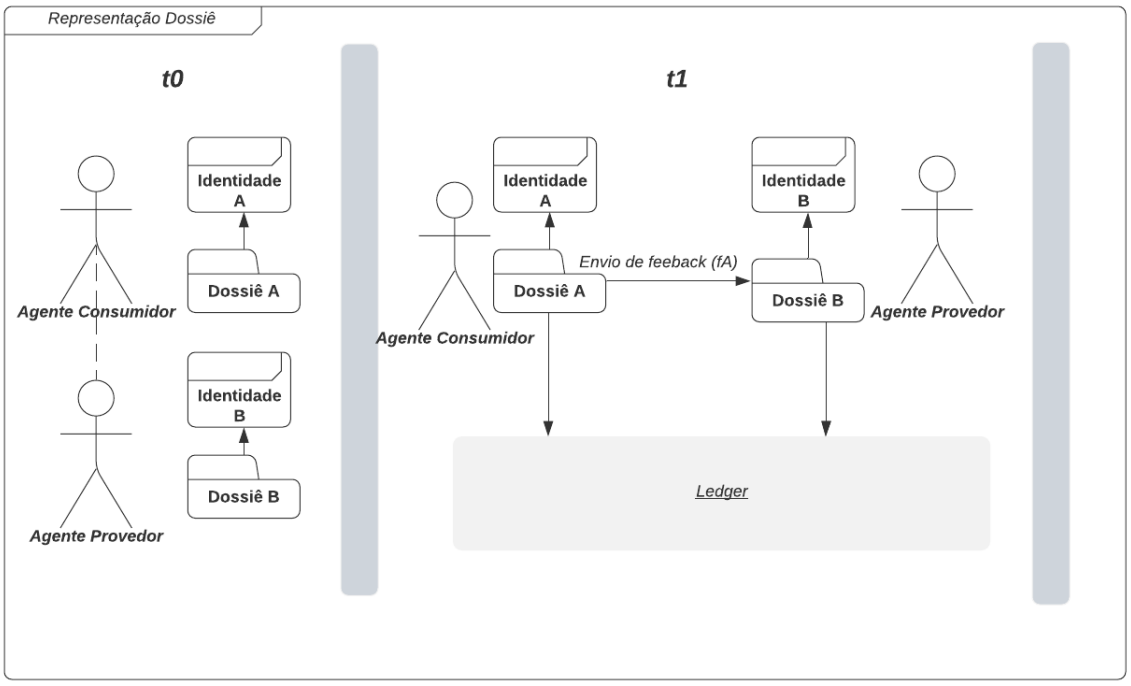

Figura 38. Cenário de *Marketplace* na interação entre agentes e os respectivos *Dossiês*.

A construção do cenário é baseada em um conjunto de *smarts contracts*, onde cada agente tem o seu próprio *smart contract*, composto por atributos, métodos e *camada de serviços* para a identidade. A construção da aplicação desse ambiente é apresentada a seguir. No entanto, deve-se notar que a ação de dar ou permitir o consentimento é registrada na rede *blockchain*, em conjunto com o compromisso estabelecido entre os agentes na troca das informações.

6.1.3 Representação dos Agentes

O agente é o elemento central da aplicação cujo comportamento representa as ações as quais a aplicação realiza. Nas *Tabelas 9, 10* e *11* são mostradas as representações das entidades da aplicação com os respectivos atributos:

1) Agente

Tabela 9. Representação da estrutura do Agente

Campo	Descrição
Id	*Hash* que representa de modo único o Agente
Nome	Nome do Agente
Sobrenome	Sobrenome do Agente
Email	E-mail do Agente
CPF	Identificação por CPF
Data Criação	Data de criação do agente na estrutura do contrato

2) *Dossiê*

Tabela 10. Representação da estrutura do *Dossiê*

Campo	Descrição
Avaliador	Endereço do Agente avaliador.
Avaliado	Endereço do agente que recebeu a avaliação.
Tipo de Serviço	Tipo de serviço prestado.
Descrição	Descrição do tipo de serviço contrato.
Feedback	Lista contendo os *feedbacks* recebido pelo Agente.
Data Criação	Data de criação do *Dossiê*

3) Identidade digital *Auto Soberana*

Tabela 11. Representação da estrutura Identidade Auto Soberana do Agente.

Campo	Descrição
Id	*Hash* da identidade digital do Agente
Aprovar Identidade	Hash de verificação se a identidade foi aprovada

O relacionamento entre as entidades segue mapeada na *Figura 39*, onde é mostrada a relação existente entre *Agentes*, *Dossiê* e *identidade digital Auto Soberana*.

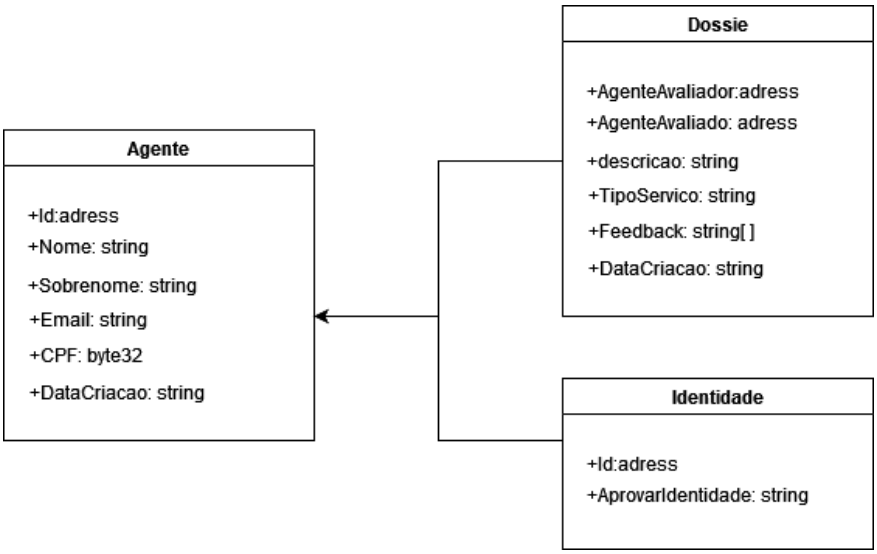

Figura 39. Representação da estrutura de entidades *Agente, Dossiê e Identidade*.

6.2 Arquitetura da aplicação

A seguir é apresentada a aplicação com aos respectivos elementos, ambos validados dentro de estruturas de *smarts contracts*, cujos *atributos* e *métodos* são representados por meio da linguagem de programação *Solidity*[10] utilizados na construção de *smarts contracts*.

6.2.1 Fluxo dos dados

Para a construção dos fluxos de dados da solução foram definidos os fluxos em relação a:

I. *Criação da estrutura Dossiê: na Figura 40 é* apresentado o fluxo de dados que resulta na criação do *Dossiê* e a inserção dentro do *blockchain.* Para a inserção dos dados do Agente dentro do *Ledger*, utiliza-se a interface da *Metamask*[11] que é o meio para validar um *smart contract* por meio de uma *carteira digital*. Após essa etapa temos a estrutura *Dossiê* já criada com a possibilidade de visualização dos *feedbacks* recebidos pelos agentes, além disso foi acrescentado a possibilidade de *verificar a identidade* do Agente.

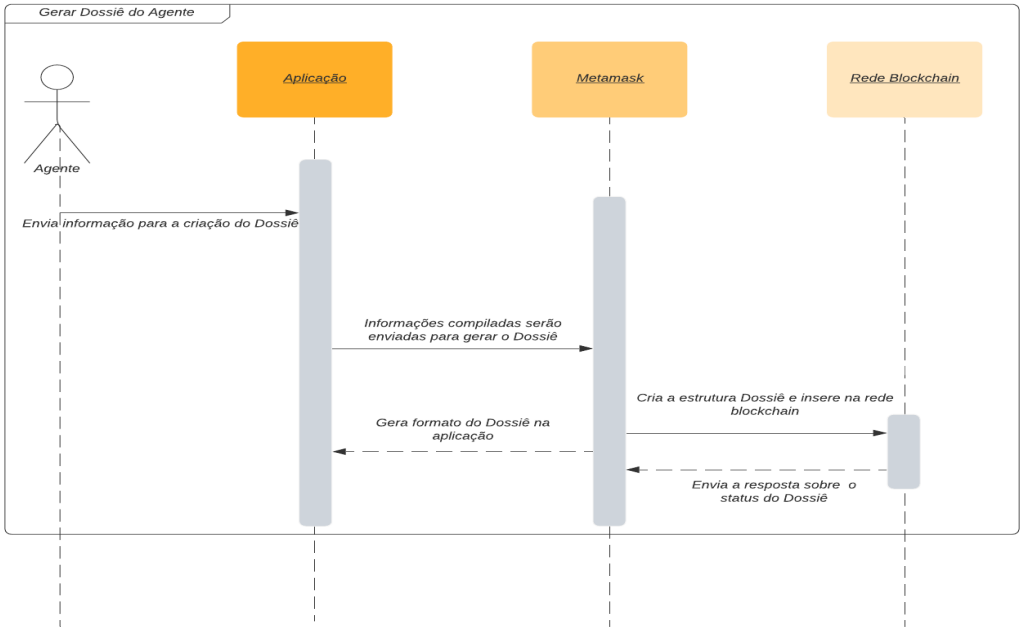

Figura 40. Fluxo de dados para criação da estrutura *Dossiê* na rede *blockchain*

A seguir, a Figura 41 representa um *smart contract* da estrutura *Dossiê*, utilizando a linguagem *Solidity*. Essa estrutura mostra os atributos e métodos que compõe a estrutura *Dossiê*.

[10] https://soliditylang.org/
[11] https://metamask.io/

```
pragma solidity ^0.6.3;

contract Dossier {
    struct Feedback {
        address agenteAvaliador;
        address agenteAvaliado;
        string descricao;
        string TipoServico;
        uint256 feedback;
        string DataCriacao;
    }

    struct Dossier {
        mapping(uint256 => Feedback) feedback;
        uint256 feedbackCounter;
    }

    struct Authorization {
        address applicant;
        uint256 authorization;
    }

    struct Authorizations {
        mapping(uint256 => Authorization) authorization;
        uint256 authorizationCounter;
    }

    mapping(address => Dossier) dossiers;  mapping(address => Authorizations) authorizations;
    address[] public dossiersAddresses;
    address[] public agentsAddresses
```

Figura 41. Estrutura do *smart contract* do Agente no formato da linguagem *Solidity*

Para a inserção dos dados do *Agente* dentro do *Ledger*, como já dito, utiliza-se a interface da *Metamask* que é o meio para validar o *smart contract* por meio de uma carteira digital. Além disso, acrescentou-se a possibilidade de *verificar a identidade* do *Agente* cuja descrição é apresentada nos próximos tópicos. Criação da identidade digital *Auto Soberana* do *Agente* (cf. a *Figura 42*) é feita utilizando o *Framework* da *uPort* (ver descrição na Seção 4.6.1).

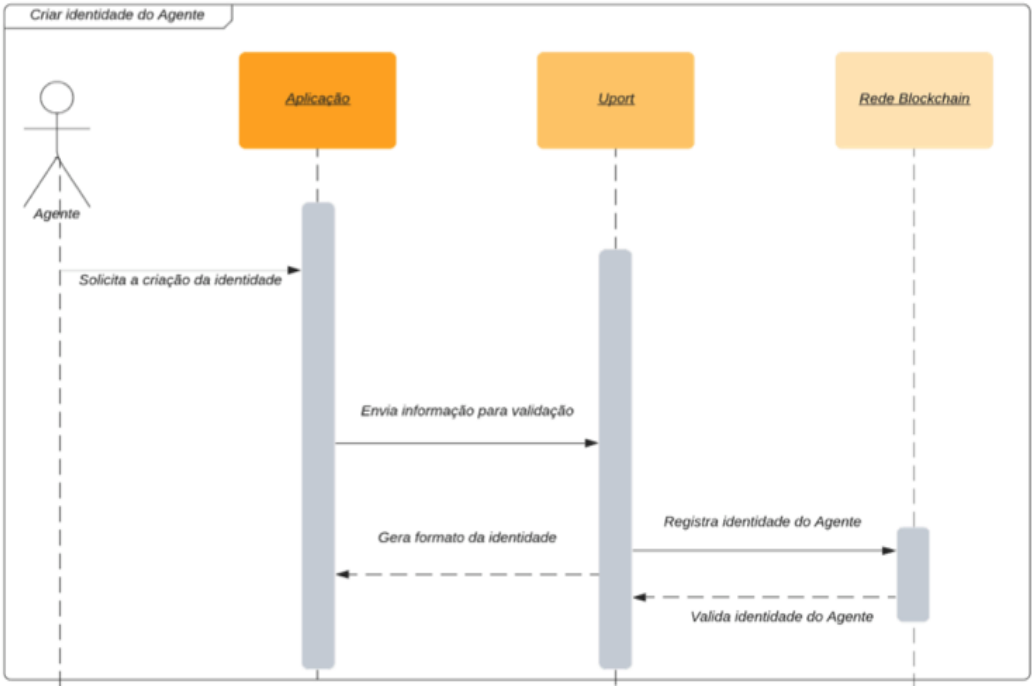

Figura 42. Fluxo de dados para criar a identidade do *Agente*.

1. O agente necessita criar uma identidade como ponto de partida e para isso envia uma requisição para o *webservices* da *uPort* para criar a identidade *Auto Soberana*.
2. A aplicação/agente com a posse dos dados envia uma requisição para que as credenciais sejam criadas e inseridas na rede *blockchain*.
3. Uma vez criadas e inseridas as novas credenciais na rede *blockchain*, o serviço da *uPort* envia uma requisição com a resposta para a aplicação.
4. Nesse momento é gerado um validador, no formato de um *qrcode* e após a leitura do mesmo as informações do agente são exibidas, podendo ser compartilhadas na troca e no uso de serviços entre agentes.
5. A identidade do Agente é um conjunto de *smart contract* desenvolvido sobre a linguagem *Solidity*. A *Figura 43* representa a construção da identidade do Agente no formato do *smart contract*.

```
pragma solidity ^0.6.3;

contract IssuerRegistry {
    mapping(address=>bool) public isIssuer;
    mapping(address=>bool) public isApprovingAuthority;
    mapping(address=>bytes32) public issuerId;
    event IssuerApproved(address indexed issuer, address indexed authority);
    event IssuerRevoked(address indexed issuer, address indexed authority);

    constructor (address[] memory authorities) public {
        for (uint256 i = 0; i < authorities.length; ++i) {
            isApprovingAuthority[authorities[i]] = true;
        }
    }
    modifier onlyAuthority {
        require(isApprovingAuthority[msg.sender], "You must be an authority.");
        _;
    }
    function approve(address issuer, bytes32 id) public onlyAuthority {
        require(!isIssuer[issuer], "Already an issuer.");
        isIssuer[issuer] = true;
        issuerId[issuer] = id;
        emit IssuerApproved(issuer, msg.sender);
    }
    function revoke(address issuer) public onlyAuthority {
        require(isIssuer[issuer], "Not an issuer.");
        isIssuer[issuer] = false;
        delete issuerId[issuer];
        emit IssuerRevoked(issuer, msg.sender);
    }
}
```

Figura 43. Estrutura do *smart contract* da identidade *Auto Soberana* do *Agente*.

O *smart contract*, denominado *IssuerRegistry*, representa a construção da identidade digital *Auto Soberana*. Na execução do *smart contract*, a entidade identidade é criada e pode ser enviada para qualquer agente. Dentro da plataforma *uPort*, existe um método, denominado *uport-credentials*, que é utilizado na geração dos pares de chaves dentro da rede *Ethereum.* Esse método segue o padrão de geração de chaves de acordo as orientações da *ERC-1056*[12]. O método abaixo implementa o processo de requisição para a criação da identidade:

[12] https://eips.ethereum.org/EIPS/eip-1056

```
const { Credentials } = require('uport-credentials');
Credentials.CreateIdentity();

Attestation Creator Service running, open at https://efa8-2001-1284-f019-ea87-7410-2289-d507-
2c08.ngrok.io

 ------------------------------------------------------------
 Encoded Attestation Sent to User (Signed JWT)
 ------------------------------------------------------------

eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NkstUiJ9.eyJpYXQiOjE2MzYyMDkxNDYsImV4cCI6MTYzNjIwOTE2OTQxMywic3ViIjoiZGlk
OmV0aHI6MHg0MmYwMTY1ZDdlMTVhMGE3Y2EwMmRlMTEyYmE3OWE1YjY0ZDFhODVkIiwiY2xhaW0iOnsiQWdlbnRlIjp7IlRpcG8iOiJJb
nZlc3RpZG9yIiwiU2l0dWHDp8OjbyI6IlJlY29tZW5kYWRvIiwiUGVyZmlsIjoibW9kZXJhZG8ifX0sImlzcyI6ImRpZDpldGhyOjB4MT
lhNzRlYzIxNTk4ZDUzZjgyNmMyNWI1NzMyNWIzYzVmY2RhMTJlOCJ9.oSv6lWZAj_SFhgSGlcdOcVKxn5M__2ObJdPv2SihWYhz-
SB4RK1ArIvUr3sW-zahLRxpixeSYQvTFuTVFUIungE
 ------------------------------------------------------------
 Decoded Attestation Payload of Above
 ------------------------------------------------------------

{
  header: { typ: 'JWT', alg: 'ES256K-R' },
  payload: {
    iat: 1636209146,
    exp: 1636209169413,
    sub: 'did:ethr:0x42f0165d7e15a0a7ca02de112ba79a5b64d1a85d',
    claim: { Agente: [Object] },
    iss: 'did:ethr:0x19a74ec21598d53f826c25b57325b3c5fcda12e8'
  },
  signature: 'oSv6lWZAj_SFhgSGlcdOcVKxn5M__2ObJdPv2SihWYhz-SB4RK1ArIvUr3sW-zahLRxpixeSYQvTFuTVFUIungE',
  data:
'eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NkstUiJ9.eyJpYXQiOjE2MzYyMDkxNDYsImV4cCI6MTYzNjIwOTE2OTQxMywic3ViIjoiZGl
kOmV0aHI6MHg0MmYwMTY1ZDdlMTVhMGE3Y2EwMmRlMTEyYmE3OWE1YjY0ZDFhODVkIiwiY2xhaW0iOnsiQWdlbnRlIjp7IlRpcG8iOiJJ
bnZlc3RpZG9yIiwiU2l0dWHDp8OjbyI6IlJlY29tZW5kYWRvIiwiUGVyZmlsIjoibW9kZXJhZG8ifX0sImlzcyI6ImRpZDpldGhyOjB4M
TlhNzRlYzIxNTk4ZDUzZjgyNmMyNWI1NzMyNWIzYzVmY2RhMTJlOCJ9'
}
 ------------------------------------------------------------
Push notification with attestation sent, will recieve on client in a moment
```

O resultado de envio da requisição *credentials* corresponde a geração de um *qrcode* (cf. a *Figura 44*), cuja função é gerar uma identidade dentro da rede *Ethereum*.

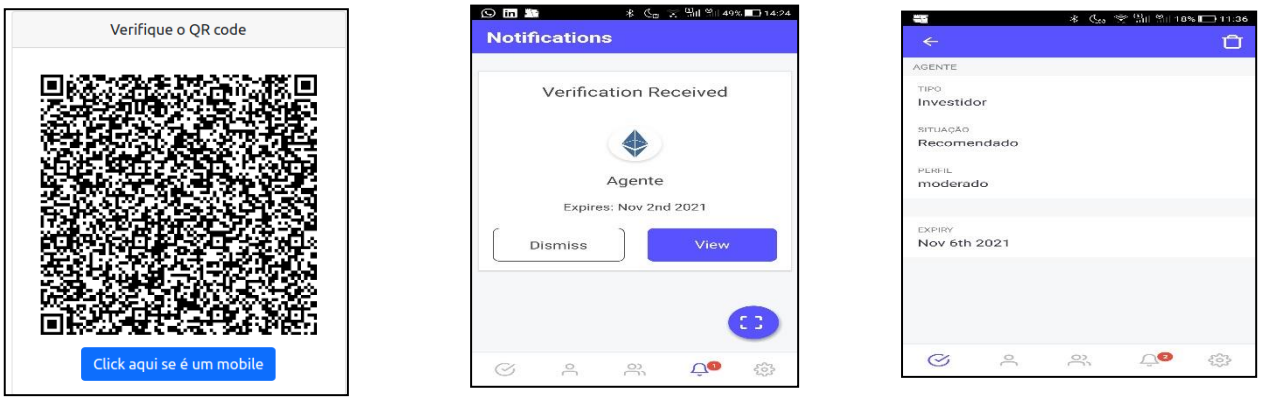

Figura 44. Qrcode para gerar a criação da *Identidade* do *Agente*.

Após a leitura do *qrcode* é gerado uma notificação de criação da identidade do Agente. A identidade *Auto Soberana* é criada e nela consta informações que identifica o agente nas transações as quais irá realizar. Há um conjunto de *atributos* que representam esse agente, no exemplo da *Figura 44*, o agente é do tipo investidor com perfil moderado para ativos. Por outro lado, em outras situações é necessário *atestar* a validade da *Identidade* do *Agente*, nesse caso deve-se:

I. Atestar a identidade digital *Auto Soberana* do *Agente* – é o processo de atestar se uma identidade é valida, que inicia com uma solicitação para as *credenciais* já criadas.

II. A credencial é identificada por seu título e chave, já gerada e utilizada por seu criador. O retorno da chamada é a verificação da *credencial* originada no servidor.

Figura 45. Verificar credencial da *Identidade* do *Agente*.

O código abaixo representa o método requisição da *credencial* da *Identidade* do *Agente* no formato de um *token*.

```
Requestor Service running, open at https://5147-2001-1284-f019-ea87-7410-2289-d507-2c08.ngrok.io
 ------------------------------------------------------------
 Encoded Request URI to send to uPort Client (Signed JWT Wrapped with URI)
 ------------------------------------------------------------
eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NkstUiJ9.eyJpYXQiOjE2MzYyMTE2NjMsImV4cCI6MTYzNjIxMjI2MywidmVyaWZpZWQiOlsi
QWdlbnRlI10sImNhbGxiYWNrIjoiaHR0cHM6Ly81MTQ3LTIwMDEtMTI4NC1mMDE5LWVhODctNzQxMC0yMjg5LWQ1MDctMmMwOC5uZ3Jva
y5pby9jYWxsYmFjayIsInR5cGUiOiJzaGFyZVJlcSIsImlzcyI6ImRpZDpldGhyOjB4MTk1ZmIyOGU1YTg4YTE1YjIxMWZhYTRmMzVhNz
Q1OTBmNjI5ZmU4OCJ9.QKbNYbNpuIHot3_HbFwK5az0BFAfuhaqu6Ncvgk0Q5pxQ6l4fENXygfbn9qF695YouFmTumHS9Iic2Jom14Shg
A
 ------------------------------------------------------------
 Decoded Request Token
 ------------------------------------------------------------
{
  header: { typ: 'JWT', alg: 'ES256K-R' },
  payload: {
    iat: 1636211663,
    exp: 1636212263,
    verified: [ 'Agente' ],
    callback: 'https://5147-2001-1284-f019-ea87-7410-2289-d507-2c08.ngrok.io/callback',
    type: 'shareReq',
    iss: 'did:ethr:0x195fb28e5a88a15b211faa4f35a74590f629fe88'
  },
  signature: 'QKbNYbNpuIHot3_HbFwK5az0BFAfuhaqu6Ncvgk0Q5pxQ6l4fENXygfbn9qF695YouFmTumHS9Iic2Jom14ShgA',
  data:
'eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NkstUiJ9.eyJpYXQiOjE2MzYyMTE2NjMsImV4cCI6MTYzNjIxMjI2MywidmVyaWZpZWQiOls
iQWdlbnRlI10sImNhbGxiYWNrIjoiaHR0cHM6Ly81MTQ3LTIwMDEtMTI4NC1mMDE5LWVhODctNzQxMC0yMjg5LWQ1MDctMmMwOC5uZ3Jv
ay5pby9jYWxsYmFjayIsInR5cGUiOiJzaGFyZVJlcSIsImlzcyI6ImRpZDpldGhyOjB4MTk1ZmIyOGU1YTg4YTE1YjIxMWZhYTRmMzVhN
zQ1OTBmNjI5ZmU4OCJ9'
}
a user connected
```

1. *Da solicitação*, a resposta é um *token JWT* assinado, que pode ser usado para verificar a assinatura.
2. *Das assinaturas*, as credenciais são incluídas no *token*, que podem ser verificadas e comprovadas para uso em cada tipo de aplicação.
3. *Da aplicação*, o método *requestCredential* é a função responsável pelo envio da solicitação para a estrutura a *uPort* (cf. a *Figura 44*).
4. Da leitura do *qrcode*, os atributos da *Identidade* do *Agente* são identificados na aplicação:

```
Credential Requested
 ------------------------------------------------------------
{
  iat: 1636209146,
  exp: 1636209169413,
  sub: 'did:ethr:0x42f0165d7e15a0a7ca02de112ba79a5b64d1a85d',
  claim: {
    Agente: {
      Tipo: 'Investidor',
      'Situação': 'Recomendado',
      Perfil: 'moderado'
```

Caso a identidade esteja na situação *inválida* ou *expirada*, o *Agente* deve gerar uma nova identidade. Aqui é importante frisar que todas as alterações na *Identidade* são registradas por meio dos *hashes* das transações na rede *blockchain* para garantir a rastreabilidade de todas as operações realizada pelo *Agente*.

6.3 Considerações finais do Capítulo

Neste Capítulo mostrou-se, a partir de um cenário simples de aplicação, a relação de troca de informação entre estruturas privadas. Nessa dinâmica, cada troca segue um protocolo, com objetivo de assegurar a rastreabilidade das informações. Em relação a prototipação, buscou-se utilizar uma plataforma real desenvolvida sobre a rede *blockchain* da *Ethereum*, com dados fictícios de usuários. Além disso, buscou-se apresentar as premissas do modelo de identidade digital *Auto Soberana*, tanto no processo de gerir essa identidade, como também na ação de atestar a validade das credenciais, nas ações de compartilhamento de informações entre agentes.

7. Discussão e conclusões

Nesse capítulo, discorreu-se sobre a *identidade digital Auto Soberana* como modelo para criar e gerenciar identidades em ambientes de distribuídos, em especial quando construído com base na tecnologia *blockchain*. Neste cenário, em particular, utilizou-se, como plataforma de experimentação a rede *Ethereum*. Esse esforço, permitiu-nos mostrar a consecução do objetivo geral, ao colocar de forma prática como agentes de software podem ter o controle sobre a sua própria *identidade digital*. O principal ganho desta integração, considerando a natureza agentes, está em assegurar o controle dos dados sensíveis de forma *descentralizada*, mantendo a responsabilidade sobre os dados com o *agente—proprietário dos dados—*, seguindo a linha da criação de uma *identidade digital* ou da verificação da validade dessa identidade em relação a serviços prestados, garantindo desse modo as propriedades de *imutabilidade, rastreabilidade* e *segurança*.

Assim, ao olharmos pela *perspectiva do usuário,* esse seria capaz de ceder o acesso pessoal aos seus próprios dados, como também monitorar quem tem acesso a eles e o como os dados estão sendo utilizados. A título de exemplo, sendo o agente provedor de serviços um banco, a contratação do serviço começaria com a verificação das identidades digitais cujo controle está em cada agente. Em seguida, com as identidades digitais validadas, o *agente do tipo banco* ofereceria os serviços disponíveis para o *usuário*. Contudo, é importante salientar que para cada serviço a ser contratado há protocolos bem-estabelecidos. Entende-se aqui como *protocolo* as regras estabelecidas para execução da interação. Nessa arquitetura, estabelece-se que há um conjunto de protocolos, cujos quais assumem a forma de conjunto de *smarts contracts*. Nos *smarts contracts* encerram as condições legais para que as transações possam ser realizadas, e à medida que os relacionamentos entre os agentes se fortalecem novos tipos de contratos vão sendo inseridos na base de dados.

Há, portanto, uma base de dados—descrevendo os contratos—e os agentes interagindo de acordo com os contratos pré-estabelecidos. Assim, ao iniciar a contratação de um serviço, previamente verifica-se no servidor da aplicação se já existe o tipo de contrato para aquela solicitação. Se já existe baixa-se o contrato e segue a contratação do serviço. É importante enfatizar que em cada contrato existe uma sessão denominada de identificação.

O agente tem a capacidade de responder um conjunto de perguntas dentro de um *link* confiável. No caso em ilustrativo, o agente *Banco* possivelmente buscará saber mais sobre o

agente solicitante do empréstimo. O agente pode responder mais sobre si, já que isso denota mais sobre a própria identidade desse agente. A transação, portanto, terminará com a atualização do *Dossiê* de cada agente e a inserção do último *hash* dentro da aplicação *blockchain*.

Há um potencial uso para a monetização do uso de dados, pois tendo o usuário o controle dos seus dados, poderão ser criados procedimentos para possibilitar a busca por uma remuneração, no momento de compartilhamento de dados entre terceiros. Essa mudança reforça a necessidade de garantir transparência de acesso, bem como uma forma de maximizar benefícios entre partes interessadas. Em resumo, o ganho consiste em garantir interações seguras entre agentes, sem a intermediação de entidades centralizadoras ou provedoras, denominadas *terceira-parte*. A abordagem apresentada fortalece significativamente o usuário quanto a transparência e o controle de dados.

Nessa linha de apresentação é importante olhar para *perspectiva dos agentes institucionais*, a exemplo dos provedores de serviços, já que o trabalho pode ajudar a facilitar a conformidade em relação as exigências das legislações de proteção aos dados, em especial com a *LGPD* no Brasil ou a *GDPR* na Europa. Com o consentimento dado pelo usuário permite o fortalecimento da transparência no uso e manipulação dos dados. Esse incentivo abre novas perspectivas de negócios, tanto por meio da monetização da venda de dados como da própria validação desses dados. Nesse contexto, a possibilidade de comprar dados de clientes, como também de usuários dos concorrentes, fornece uma oportunidade significativa para as empresas expandirem e melhorarem as prestações dos serviços, pois possibilitam a geração de *insights* sobre seus clientes, além da oportunidade de descobrir novos mercado.

Quanto a arquitetura do sistema, buscou-se construí-la delegando responsabilidades para cada componente da aplicação. Indo, portanto, além dos modelos tradicionais baseados apenas na relação de cliente/servidor, ou seja, não se trata somente de um sistema de interação entre agentes com os papéis cliente e provedor de serviços. Vai além, já que é construído a partir do paradigma descentralizado, sob o modelo *identidade digital Auto Soberana* que faz o uso da própria estrutura para distribuir informações e descentralizar dados. Desse modo, o próprio recurso de descentralização, quando validado dentro das cadeias de blocos, permite a rastreabilidade das transações, ocorridas por todos os nós participantes da cadeia. Essa estratégica pode identificar agentes não-honestos ou hostis pela leitura dos *hashes* dentro da cadeia de blocos. Desse modo, o ambiente administrado pelo modelo *identidade digital Auto Soberana* quebra o paradigma de disposição das informações sensíveis dos indivíduos encontrados em plataformas *online*. Deve-se notar que o modelo *Auto Soberano* outorga ao

indivíduo o poder de mostrar as informações necessárias por *contexto de aplicação*. Pode ser que usuário não tenha interesse, ao se conectar a um determinado serviço, mostrar todo histórico de suas transações, pois *no contexto da aplicação* essa decisão de autorizar ou não a visualização fica a critério do usuário.

Por fim, buscou-se com esse trabalho entender como o modelo de identidade digital *Auto Soberana* atuaria em conjunto com a estrutura *Dossiê*. Desse modo, além da estrutura de armazenamento local e de controle de informações, adicionou-se uma camada *a mais* em relação os recursos para gerar, verificar e/ou compartilhar uma identidade em função do contexto da aplicação; o contexto da aplicação ajuda a definir a minimização da exposição. É importante salientar que tanto as transações que dão origem ao *Dossiê* ou identidade do *Agente*, quanto as demais transações representam registros ou solicitações de informações que ocorrem por meio de micro pagamentos dentro da rede *Ethereum*.

7.1 Trabalhos futuros

A pesquisa feita até o momento deixa em aberto várias oportunidades para trabalhos futuros, listadas como segue:

1. avaliar o uso em grandes sistemas com o objetivo verificar o comportamento e a possibilidade de escalar a aplicação do modelo identidade digital *Auto Soberana* em conjunto com a estrutura de dados *Dossiê*.
2. avaliar estratégias que possibilitem novas interações entre diferentes tipos de entidades, em especial, em relação as questões que abordam a troca de informações sensíveis e das ações de consentimento asseguradas pela *LGPD*.
3. avaliar estratégias de transferência segura de dados com uso de algoritmos de criptografias entre provedores de repositórios de dados fora da cadeia com integração de serviços. Há a necessidade de preparar uma especificação detalhada descrevendo várias interações entre as partes interessadas do Sistema de uma forma inequívoca.
4. avaliar estratégias seguras que permitam que a credenciais ou certificados digitais criados a partir do modelo de identidade digital *Auto Soberana* tenham o mesmo valor de emissão das credenciais de identidade, carteiras de motorista, diplomas ou qualquer outro documento emitido por entidade certificadora, desde que as credenciais estejam de acordo com o padrão estabelecido para credenciais baseadas no modelo de identidade *Auto Soberano* atuando dentro de uma rede *blockchain*.

8. Referências

ABID, A, Cheikhrouhou, S, Kallel, S, Jmaiel, M. NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. *Softw Pract Exper*. 2021.

ABRAHAM, A K. Theuermann and E. Kirchengast, "Qualified eID Derivation Into a Distributed Ledger Based IdM System,". IEEE. 2018.

ABRAHAM, A, S. More, C. Rabensteiner and F. Hörandner, "Revocable and Offline-Verifiable Self-Sovereign Identities,". IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications TrustCom. 2020.

ADELINDE M. Uhrmacher and Danny Weyns. Multi-Agent Systems: Simulation and Applications. Computational analysis, synthesis, and design of dynamic models series. 2009.

AGUIRRE, E., Mahr, D., Grewel, D., Ruyter, K. D., & Wetzels, M. Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. Journal of Retailing, 2015.

AHMED, K. A. M., S. F. Saraya, J. F. Wanis and A. M. T. Ali-Eldin, "A Self-Sovereign Identity Architecture Based on Blockchain and the Utilization of Customer's Banking Cards: The Case of Bank Scam Calls Prevention,". 2020.

ALBOAIE, Sînică, Ursache, Nicu-Cosmin & Alboaie, L. Self-Sovereign Applications: return control of data back to people. Procedia Computer Science.2020.

AL-KHOURI, Ali. Data Ownership: Who Owns My Data? International Journal Of Management & Information Technology. 2. 1-8. 2012.

ALLEN, C. "The path to self-sovereign identity." [Online]. In: https://github.com/WebOfTrustInfo/self-sovereign-identity. Acessado em: 11-2021.

ALZAHRANI, Bander. An Information-Centric Networking Based Registry for Decentralized Identifiers and Verifiable Credentials. IEEE Access. PP. 1-1. 2020

ANDRIEU, Joe. A Technology-Free Definition of Self-Sovereign Identity. In https://github.com/WebOfTrustInfo/self-sovereign-identity. 2016. Acessado em: 11-2021

ARORA, C. Digital health fiduciaries: protecting user privacy when sharing health data. Ethics Inf Technol 21, 181–196. 2019.

BAARS, D.S. Towards self-sovereign identity using blockchain technology.Thesis.. University of Twente. 2016.

BADICA, Costin & Budimac, Zoran & Burkhard, Hans-Dieter & Ivanovic, Mirjana. Software Agents: Languages, Tools, Platforms. Comput. Sci. Inf. Syst. 2011.

BADREDDINE, Wiem & Zhang, Kaiwen & Talhi, Chamseddine. Monetization using Blockchains for IoT Data Marketplace. 2020.

BANDARA, E., Liang, X., Foytik, P., Shetty, S., Hall, C., Bowden, D., Ranasinghe, N., De Zoysa, K. A blockchain empowered and privacy preserving digital contact tracing platform. 2021.

BASTIAN Könings. User-centered Awareness and Control of Privacy in Ubiquitous Computing. 2015.

BECKER, M. Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. Ethics and Information Technology, 21 4., pp. 307-317. 2019.

BIGHAM, John & Du, Lin. Cooperative Negotiation in a Multi-Agent System for Real-Time Load Balancing of a Mobile Cellular Network. Proceedings of the Interantional Conference on Autonomous Agents. 2003.

BOKKEM ,van, Dirk & Hageman, Rico & Koning, Gijs & Nguyen, Tat Luat & Zarin, Naqib.Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. 2019.

BOUWENS, Maarten. Towards more foundational humanitarian Self-Sovereign Identity systems. 2020.

BOWIE, N. E., & Jamal, K. Privacy rights on the internet: self-regulation or government regulation. 2006.

BRENNER,Walter, H. Wittig, and Rudiger Zarnekow. Intelligent Software Agents: Foundations and Applications 1st. ed... Springer-Verlag, Berlin, Heidelberg.1998.

BUCCAFURRI, Francesco & Rosaci, Domenico & Sarnè, Giuseppe M. L. & Palopoli, Luigi. SPY: A MULTI-AGENT MODEL YIELDING SEMANTIC PROPERTIES. 44-53. 2001.

CAMERON, Kim. Architect of Identity, Microsoft Corporation. [Online] In: https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md. 2005. Acessado em: 11-2021.

CANEDO, Edna Dias e Ribeiro, Renato. Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security. 2020.

_____, Artur Potiguara, Fernanda Potiguara Carvalho, and Pedro Henrique Potiguara Carvalho. Big Data, Anonymisation and Governance to Personal Data Protection. Association for Computing Machinery, New York, NY, USA, 2020.

CAO, Yuan, Lin Yang, "A survey of Identity Management technology,". IEEE International Conference on Information Theory and Information Security, 2010.

CASTELLS, Manuel. O poder da identidade. Tradução Klauss Brandini Gerhardt. 2. ed. São Paulo: Paz e Terra, 2018. 530p. (A Era da Informação: economia, sociedade e cultura, 2).

_____. A sociedade em rede. São Paulo: Paz e Terra, 2005

CARVALHO, Artur & Carvalho, Fernanda & Canedo, E.D. & Carvalho, Pedro. Big Data, Anonymisation and Governance to Personal Data Protection. 185-195. 2020.

CHEN J, Ge H, Li N, Proctor RW. What I Say Means What I Do: Risk Concerns and Mobile Application-Selection Behaviors. Human Factors. 2021.

CHO, Hichang & Roh, Sungjong & Park, Byung. Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. Computers in Human Behavior. 2019.

DE FILIPPI, Primavera; Fennie Wang. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion Journal Article published in Frontiers in Blockchain volume 2. 2020.

DECEW, J. In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Cornell University Press, Ithaca. 1997.

DER, Uwe, S. Jähnichen and J. Sürmeli. Self-sovereign identity Opportunities and challenges for the digital revolution. 2017.

DIB, Omar & Toumi, Khalifa. Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions. Annals of Emerging Technologies in Computing. 2020.

DORRI, Ali & Kanhere, Salil & Jurdak, Raja. Multi-Agent Systems: A survey. IEEE 2018.

DURNELL, E., Okabe-Miyamoto, K., Howell, R.T., Zizi, M. Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale. 2020.

EL MALIKI, T., & Seigneur, J.-M. Online Identity and User Management Services. Computer and Information Security Handbook, 459–484. 2013.

FABER, Benedict & Michelet, Georg & Weidmann, Niklas & Mukkamala, Raghava Rao & Vatrapu, Ravi. BPDIMS:A Blockchain-based Personal Data and Identity Management System. 2019.

FAN, Pengfei et al. "Identity Management Security Authentication Based on Blockchain Technologies." Int. J. Netw. Secur. 2019.

FERDOUS, M. S, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE. 2019.

FISHER Michael, Anthony Hepple: Executing Logical Agent Specifications. Multi-Agent Programming, Languages, Tools and Applications. 2009.

NASCIMENTO, Marcos Pereira; Franciscon, Eduardo; Granatyr, Jones; Weffort, Marcos, Lessing, Otto , Scalabrin, Edson. A Systematic Literature Review of Blockchain Architectures Applied to Public Services. 2019.

FREUND, Andrea. “Automated, Decentralized Trust: A Path to Financial Inclusion.”.2018.

GATTI DE BAYSER, Maira & Gatti, C & Lucena, Carlos & Briot, Jean-Pierre.. On fault tolerance in law-governed multi-agent systems. 2006.

GDPR. Ico.org.uk. Guide to the general data protection regulation [Online]. Disponível em : https://ico.org.uk/for-organisations/guide-to-data-protection/. 2020.

GEBRESILASSIE S. K., J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair and Z. Cui, "Distributed, Secure, Self-Sovereign Identity for IoT Devices," 2020 IEEE 6th World Forum on Internet of Things. 2020.

GERMAN BLOCKCHAIN ASSOCIATION. Self-sovereign Identity: A position paper on blockchain enabled identity and the road ahead. Group of the German Blockchain Association. In: https://bundesblock.de/ .2018.

GILANI, K., E. Bertin, J. Hatin and N. Crespi, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data," 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services BRAINS., 2020.

GILANI, K., E. Bertin, J. Hatin and N. Crespi, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data,". 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services BRAINS. 2020.

GRANATYR J., V. Botelho, O. R. Lessing, E. E. Scalabrin, J.-P. Barth`es, and F. Enembreck, “Trustand reputation models for multiagent systems,” ACM Computing Surveys CSUR., vol. 48, no. 2, p. 27. 2015.

GRÜNER,A., A. Mühle and C. Meinel, "An Integration Architecture to Enable Service Providers for Self-sovereign Identity," 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), 2019, pp. 1-5, doi: 10.1109/NCA.2019.8935015.

GULATI, Himani & Huang, Chin-Tser. Self-Sovereign Dynamic Digital Identities based on Blockchain Technology. 2019.

HANG, Lei & Kim, Do-Hyeun. (2019). SLA-Based Sharing Economy Service with Smart Contract for Resource Integrity in the Internet of Things. Applied Sciences. 9. 10.3390/app9173602.

HAMER, T., Kerry Taylor, Kee Siong Ng, Alwen Tiu. Private Digital Identity on Blockchain. Proceedings of the Blockchain enabled Semantic Web Workshop BlockSW. and Contextualized Knowledge Graphs CKG. Workshop co-located with the 18th International Semantic Web Conference, BlockSW/CKG@. ISWC. 2019.

HADDOUTI, S. E. and M. D. Ech-Cherif El Kettani, "Analysis of Identity Management Systems Using Blockchain Technology". International Conference on Advanced

Communication Technologies and Networking (CommNet), 2019, pp. 1-7, doi: 10.1109/COMMNET.2019.8742375. 2019.

HARDJONO,Thomas; David L. Shrier; Alex Pentland, "APPENDIX A PERSONAL DATA: THE EMERGENCE OF A NEW ASSET CLASS," in Trusted Data: A New Framework for Identity and Data Sharing , MIT Press, 2019.

HARM, Jan-Gerrit. Creating trust through verification of interaction. Delft University of Technology.2018

HASAN, H. R. et al., "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates," in IEEE, 2020.

HAYZELDEN, Alex & Bigham, John. Agent Technology in Communications System: An Overview. The Knowledge Engineering Review. 1999.

HOEL, T., Chen, W. Privacy and data protection in learning analytics should be motivated by an educational maxim—towards a proposal. Research and Practice in Technology Enhanced Learning, 13 1., art. no. 20. 2018.

HOUTAN, B., A. S. Hafid and D. Makrakis, "A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare," in IEEE. 2020.

INOUE, Koki & Imai, Satoshi & Suzuki, Dai & Kurita, Toshihiko. Process Scheduling of Personal Identity Verification on Decentralized Trust. 2020.

IRAMINA, Aline. Rgpd V. Lgpd: Adoção Estratégica Da Abordagem Responsiva Na Elaboração Da Lei Geral De Proteção De Dados Do Brasil E Do Regulamento Geral De Proteção De Dados Da União Europeia. Revista de Direito, Estado e Telecomunicações. 2020.

JAMAL, Arshad et al. “Blockchain-Based Identity Verification System.” 2019 IEEE 9th International Conference on System Engineering and Technology ICSET. 2019

JEFFREY M. Bradshaw: Invited Talk Human-Agent Teamwork in Cyber Defense. MATES.2012.

JENNINGS, N. R., Faratin, P., Lomuscio, A. R., Parsons, S., Wooldridge, M. J., & Sierra, C. Group Decision and Negotiation, 2001.

KANNENGIESSER, Niclas & Lins, Sebastian & Dehling, Tobias & Sunyaev, Ali. Mind the Gap: Trade-Offs between Distributed Ledger Technology Characteristics. 2019.

KASSEM, Alsayed, Jamila & Sayeed, Sarwar & Marco-Gisbert, Hector & Pervez, Zeeshan & Dahal, Keshav. DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network. 2019.

KRAUS, Sarit. Automated Negotiation and Decision Making in Multiagent Environments. Lecture Notes in Computer Science. 2001.

LEE, Jeonghyuk et al. “SIMS: Self Sovereign Identity Management System with Preserving Privacy in Blockchain.” IACR Cryptol. ePrint Arch. 2019.

LESLIE, Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 1982.

LESAVRE, Loic & Varin, Priam & Mell, Peter & Davidson, Michael & Shook, James. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. 2019

LGPD: Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709 / 2018.

LIU, J., A. Hodges, L. Clay and J. Monarch, "An analysis of digital identity management systems - a two-mapping view," 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services BRAINS. 2020.

LIU, Yang & He, Debiao & Obaidat, Mohammad & Kumar, Neeraj & Khan, Khurram & Choo, Kim-Kwang Raymond. Blockchain-based identity management systems: A review. Journal of Network and Computer Applications. 2020.

LIU, Yue & Lu, Qinghua & Paik, Hye-young & Xu, Xiwei & Chen, Shiping & Zhu, Liming. Design-Pattern-as-a-Service for Blockchain-Based Self-Sovereign Identity. IEEE. 2020.

LUX, Z.A., Thatmann, D., Zickau, S. and Beierle, F. Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials. 2020.

MAIA, Rubens Dias. O conceito de identidade na filosofia e nos atos de linguagem. 2008.

MA, Shenglan & Guo, Chaonian & Wang, Hao & Hong, Xiao & Xu, Botong & Dai, Hong-Ning & Cheng, Shuhan & Yi, Ruihua & Wang, Tongsen. Nudging Data Privacy Management of Open Banking Based on Blockchain. 2018.

MELL, P. et al. “Smart Contract Federated Identity Management without Third Party Authentication Services.” Open Identity Summit. 2019.

MILBERG, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. Values, personal information privacy, and regulatory approaches. Communications of the ACM.1995.

MORELLATO, Ana Carolina Batista; DOS SANTOS, André Filipe Pereira Reid. A Capitalismo de vigilância e a lei geral de proteção de dados: Anonimização e consentimento. Revista Brasileira de Sociologia do Direito, v. 8, n. 2, p. 184-211, 2021.

MÜHLE, Alexander & Grüner, Andreas & Gayvoronskaya, Tatiana & Meinel, Christoph. A survey on essential components of a self-sovereign identity. Computer Science Review. 2018.

MUKTA, R., J. Martens, H. -y. Paik, Q. Lu and S. S. Kanhere, "Blockchain-Based Verifiable Credential Sharing with Selective Disclosure,". 2020.

NAIK, N and P. Jenkins, "Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity," 2020 7th International Conference on

Behavioural and Social Computing BESC. 2020.

_____"Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems," IEEE. 2020.
_____. Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology.2020.

NAWA, N. E., K. Shimohara and O. Katai. “Equilibrium selection in a sequential multi-issue bargaining model using evolutionary algorithms: a preliminary study.”.2001.

OTTE, Pim; Martijn de Vos, and Johan Pouwelse. Trustchain: A sybil-resistant scalable blockchain. Future Generation Computer Systems, 2017

OTHMAN, Asem & Callahan, John. The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity. 2018.

PAINE, C., Reips, U.D., Stieger, S., Joinson, A., Buchanan, T. Internet users’ perceptions of ‘privacy concerns’ and ‘privacy actions. Int. J. Hum. 2007.

PREUKSCHAT, Alex; Drummond Reed. Self-Sovereign Identity: Decentralized digital identity and verifiable credentials. Manning. 2021.

REN, Y.; Zhu, F.; Qi, J.; Wang, J.; Sangaiah, A.K. Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things. Appl. Sci. 2019.

RUDDELL, Benjamin & Cheng, Dan & Fournier, Eric & Pincetl, Stephanie & Potter, Caryn & Rushforth, Richard.. Guidance on the usability-privacy tradeoff for utility customer data aggregation. Utilities Policy. 2020.

RUSSELL, J., and P. Norvig. Artificial Intelligence: A Modern Approach. Prentice Hall, 2013.

SATOSHI, Nakamoto, email communication, In: http://satoshi.nakamotoinstitute.org/emails/cryptography. 2008.

SATYBALDY, Abylay & Nowostawski, Mariusz & Ellingsen, Jørgen. Self-Sovereign Identity Systems: Evaluation Framework. 2020.

SCAICO, O. O desenvolvimento da Identidade nas organizações evoluídas. Revista De Administração, 20(4), 42-50. In. https://www.revistas.usp.br. 1985.

SHETTY, Sachin & Liang, Xueping & Bowden, Daniel & Zhao, Juan & Zhang, Lingchen. Chapter 3: Blockchain Based Decentralized Accountability And Self Sovereignty In Healthcare Systems. 2018.

SILVA B. V. DOSSIÊ: MODELO DE CONFIANÇA PARA SISTEMAS MULTIAGENTES. Tese de Doutorado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná. 2017.

_____. Um modelo de confiança certificado baseado em assinatura digital aplicado a sistemas multiagente. Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná. 2009.

SILVA, Jefferson & Calegari, Newton & Gomes, Eduardo. After Brazil's General Data Protection Law: Authorization in Decentralized Web Applications. 2019.

_____., Milberg, S. J., & Burke, S. J. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly. 1996.

SMITH, H. J., Dinev, T., & Xu, H .Information privacy research: An interdisciplinary review. MIS Quarterly. 2011.

SMOLAK, K., Rohm, W., Knop, K., Siła-Nowicka, K. Population mobility modelling for mobility data simulation 2020.

SOLOVE, Daniel J. "A taxonomy of privacy." U. Pa. L. Rev. 154.: 477. 2005.

SOLTANI, R. A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger. pp. 1129-1136. IEEE, 2018.

_____. An, "Practical Key Recovery Model for Self-Sovereign Identity Based Digital Wallets," .2019.

_____. An, "Decentralized and Privacy-Preserving Key Management Model," 2020.

SRINIVASAN, D. L. C. Jain, Innovations in Multi-Agent Systems and Application. Springer, 2010.

STEVENS, Lars. Self-Sovereign Identities for Scaling Up Cash Transfer Projects: Designing a blockchain based digital identity system. 2018.

STOKKINK, Q. and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity,".2018.

_____, Epema, D. & Pouwelse, J.A. A Truly Self-Sovereign Identity System. 2020.

SUNYAEV, Ali. Distributed Ledger Technology. 2020.

SZABO N. Smart contracts: building blocks for digital free markets. Extropy J. Transhuman Thought, 1996.

TOBIN, Andrew; Drummond Reed. The Inevitable Rise of Self-Sovereign Identity.In. sovrin.org. 2017.

TOTH, Kalman & Anderson-Priddy, Alan. Self-Sovereign Digital Identity: A Paradigm Shift for Identity. IEEE Security & Privacy. 2019.

VASILAKOS, V, D. Ye, M. Zhang, and A. A survey of self-organization mechanisms in

multiagent systems. IEEE Trans. Syst., Man, Cybern., Syst. 2017.

VIKRAM Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. Privacy Care: A Tangible Interaction Framework for Privacy Management. 2021.

W3C Credentials Community Group. A Primer for Decentralized Identiers. [Online]. Available: https://w3c-ccg.github.io/did-primer/, 2019.

WANG, Hao & Ma, Shenglan & Dai, Hong-Ning & Imran, Muhammad & Wang, Tongsen. Blockchain-based data privacy management with Nudge theory in open banking. Future Generation Computer Systems. 2020.

WANG, H., L. Vo, F. P. Calmon, M. Médard, K. R. Duffy and M. Varia, "Privacy With Estimation Guarantees," in IEEE Transactions on Information Theory, vol. 65, no. 12, pp. 8025-8042, Dec. 2019.

WEINHARDT, Michael. Big Data: Some Ethical Concerns for the Social Sciences. Social Sciences. 2021.

WIERINGA, Jaap & Kannan, P. K. & Ma, Xiao & Reutterer, Thomas & Risselada, Hans & Skiera, Bernad. Data analytics in a privacy-concerned world. Journal of Business. 2019.

WILLIAMS, M., Nurse, J.R.C., Creese, S.Smart.Watch Out! encouraging privacy-protective behavior through interactive games. International Journal of Human Computer Studies, 132, pp. 121-137. 2019.

WOOLDRIDGE, M. An Introduction to Multiagent Systems. New York, NY, USA: Wiley, 2009.

WORD BANK. 1.1 billion 'invisible' people without ID are priority for new high level advisory council on identification for development". 2017.
_____. Technical Standards for Digital Identity: Draft for Discussion. Technical.2017.
_____. Digital identity: towards shared principles for public and private sector. 2017.

WU, D. Software agents for knowledge management: Coordination in multi-agent supply chains and auctions. Expert Systems with Applications.2001.

XIAO M., Ma Z., Li T. Privacy-Preserving and Scalable Data Access Control Based on Self-sovereign Identity Management in Large-Scale Cloud Storage. In: Wang G., Chen B., Li W., Di Pietro R., Yan X., Han H. eds. Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS. 2021.

YANG, Xiao hui & Li, Wenjie. A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers & Security. 2020.

ZYSKIND, G., O. Nathan and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Security and Privacy Workshops*, San Jose, CA, USA, 2015.