Revista Brasileira de Computação Aplicada, Abril, 2024

DOI: 10.5335/rbca.v26i1.15113
Vol. 26, Nº 1, pp. 38–49
Homepage: seer.upf.br/index.php/rbca/index

ARTIGO ORIGINAL

Uma perspectiva tecnológica para o uso de *Blockchain* na Identificação Civil: uma revisão sistemática

A technological perspective for Civil Identification with *Blockchain*: a systematic review

Naiara Motta [1,2], Joathan Lopes [2], Marcela Souza [2], Hugo Kuribayashi [2]

[1]Polícia Civil do Estado do Pará, [2]Universidade Federal do Sul e Sudeste do Pará

* {naiara.santos, joathan.slp, marcela.alves, hugo}@unifesspa.edu.br

Recebido: 17/08/2023. **Revisado:** 02/04/2024. **Aceito:** 25/04/2024.

Resumo

Após a validação do Decreto Federal nº 10.977, que define o Serviço de Identificação do Cidadão, no qual os Cartões de Identificação Geral (RGs) são numerados com base no Cadastro de Pessoa Física e expedidos com critérios de emissão uniformes para todo o território brasileiro, é de extrema importância que os estados adaptem seus sistemas de identificação. Para isso, é preciso garantir a segurança dos dados dos cidadãos e preparar todo o pessoal da administração pública. A revisão sistemática desenvolvida neste artigo tem como objetivo apresentar as possíveis aplicações do *blockchain* e as consequências do uso para a administração pública, especialmente no campo da identificação do cidadão, e apresentar seus principais usos. Com base em artigos encontrados em bases de dados como Scopus, Web of Science, IEEE Xplore e Science Direct, foram selecionados 21 artigos que tratam de *blockchain*, administração pública e identificação do cidadão por meio do método PRISMA. As principais aplicações encontradas tratavam de processamento de dados e segurança de dados públicos. Os impactos destacados foram melhoria na gestão de dados, agilidade nos serviços prestados pela administração pública, descentralização dos dados e garantia da segurança das informações. A tecnologia *Blockchain* tem o potencial de desencadear grandes mudanças na prestação de serviços públicos e nas estratégias internas do governo.

Palavras-Chave: Revisão Sistemática; *Blockchain*; Identificação Civil; Contratos Inteligentes.

Abstract

After the validation of Federal Decree No. 10977, which establishes the Citizen Identification Service to amend Law No. 7116/83, whereby General Identification Cards (RGs) are now linked to the Civil Registry (Cadastro de Pessoa Física) and issued with uniform criteria across Brazil, it is imperative for states to update their identification systems accordingly. This requires ensuring the security of citizens' data and preparing all public administration personnel. This article presents a systematic review aiming to explore potential blockchain applications and their implications for public administration, particularly in citizen identification. Twenty-one articles were selected from databases including Scopus, Web of Science, IEEE Xplore, and Science Direct, utilizing the PRISMA method. The primary applications identified focus on data processing and enhancing public data security. Notable impacts include improved data management, enhanced service agility within public administration, decentralized data storage, and bolstered information security. Blockchain technology holds significant potential to revolutionize public service delivery and governmental strategies.

Keywords: Systematic Review; Blockchain; Civil Identification; Smart Contracts.

1 Introdução

Nos termos da legislação brasileira e internacional, qualquer pessoa é dotada de personalidade, característica inerente ao homem, conceito básico da ordem jurídica, consagrado na legislação civil e nos princípios constitucionais de vida, liberdade e igualdade. Sob a perspectiva da identificação civil, a cédula/carteira de identidade ou Registro Geral (RG) é o documento nacional de identificação no território brasileiro. A partir de sua emissão, um cidadão brasileiro pode, por exemplo, garantir a expedição de diversos outros documentos. Até 2023, a legislação brasileira outorgará ao estado civil do requerente (conforme Lei nº 7.116, de 23 de agosto de 1983), a emissão deste, o que caracteriza-se atualmente em diferentes abordagens, sistemas de informação, além de requisitos e informações que devem ser prestados pelos cidadãos em cada um dos entes federativos (República Federativa do Brasil, 1983). Por outro lado, conforme Decreto Federal n. 10.977 de 23 de fevereiro de 2022, institui-se o Serviço de Identificação do Cidadão (SIC), de forma a regulamentar a Lei nº 7.116/83, e prevê a substituição do atual Sistema Nacional de Registro de Identificação Civil, através do qual RGs passarão a possuir numeração única baseada no Cadastro de Pessoas Físicas (CPF), expeditos com critérios padronizados de emissão em todo o território brasileiro (Presidência da República, 2022).

Por outro lado, apesar do Decreto n. 10.977/22 prever a expedição em formato digital do RG, observa-se que passará a vigorar a obrigatoriedade de centralização das informações de cadastro dos cidadãos junto a base de dados do SIC. De fato, diante da constante evolução da tecnologia na atualidade, uma maior rapidez e flexibilização dos processos e atividades sociais, tem sido perseguida por diversos setores, inclusive na administração pública, para agilizar processos, diminuir ou alterar algumas etapas e trazer benefícios para as pessoas e populações. Porém, cabe destacar que a gestão de informações pessoais (e privadas), sempre foi uma parte indispensável da vida e do trabalho da sociedade humana (Chen et al., 2019). Este processo, por exemplo, inclui o gerenciamento de dados que podem ser utilizados para registros de saúde, processos judiciais nas esferas civil e criminal. E, conforme a Lei n. 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes de como os dados pessoais dos cidadãos podem ser coletados e tratados, geram-se obrigações específicas para os controladores dos dados (Presidência da República, 2018). Por meio de um conjunto de procedimentos e normas, mesmo para a administração pública, a LGPD cria um conjunto de novos conceitos jurídicos, de forma a estabelecer as condições nas quais os dados pessoais (potencialmente privados e sensíveis) devem ser armazenados e manuseados.

Desta forma ressurge uma questão evidente: Como armazenar tais dados privados de forma segura? Tal dilema tem representado um relevante problema para muitas empresas e governos (Soomro et al., 2016). Ao se considerar o contexto de identificação civil, os sistemas de identificação civil no mundo evoluíram com as oportunidades criadas por diversos avanços tecnológicos, pela informatização dos governos, entre outros. Porém no cenário brasileiro, o processo de identificação civil tem permanecido fundamentalmente o mesmo nos últimos 50 anos. Este processo de atraso tecnológico causa diversos outros problemas, como dificuldade de validação, lentidão de processos, fraude, quebra de disponibilidade de informações, risco de perda dos documentos físicos, inexistência de sistemas biométricos, centralização dos dados e abertura a invasões.

Por outro lado, mesmo com a padronização do processo de expedição e utilização de sistemas informatizados à luz do Decreto n. 10.977/22, estes geralmente adotam plataformas centralizadas, baseados em arquitetura cliente-servidor, para gerenciar todas as informações deste processo. A maior desvantagem dessa arquitetura é que ela centraliza o armazenamento de dados e o esquema de permissões de acesso e modificação a estes dados, fazendo com que um usuário administrador controle a base de dados central e autorize outros usuários a acessar ou eventualmente modificar tais dados (Cui and Zhang, 2017). O risco de vazamento e adulteração de dados é alto e potencialmente catastrófico. E embora, o Decreto n. 10.977/22 preveja que as secretarias de Segurança Pública dos entes federativos serão responsáveis pela disponibilização do novo RG, há ainda um prazo de 01 (um) ano a partir da data de expedição do Decreto, até sua efetiva implementação por tais entes, para que tais órgãos estabeleçam um esquema de fornecimento do novo documento. Além disso, o RG atual permanecerá válido por até 10 (dez) anos para população de até 60 anos, o que tende a postegar os efeitos negativos gerados com o modelo atual de identificação civil no Estado brasileiro, muito embora, o novo modelo não seja capaz de superar todos os desafios relacionados.

Em adição ao exposto, os dados gerenciados por um sistema de identificação civil envolvem o armazenamento de um considerável volume de informações privadas, portanto, a divulgação de tais informações leva diretamente à segurança das pessoas envolvidas, bem como potenciais danos no acesso à funções essenciais de um município ou estado por um cidadão, como a identificação de pessoas e cadáveres, a resolução de crimes, entre outros. Desta forma, a centralização de tais dados, cria inevitavelmente um ponto único de falha, o que representa uma ameaça à preservação das propriedades da tríade Confidencialidade, Integridade e Disponibilidade (CID). Neste contexto, a tecnologia de *Blockchain* representa uma promissora alternativa neste processo, ao representar um banco de dados distribuído baseado em rede Peer-to-Peer (P2P). *Blockchain* é o resultado da integração de muitas tecnologias, que incluem protocolo P2P, mecanismos de consenso, algoritmos de criptografia, contratos inteligentes, de forma a representar minimamente uma maneira diferente de armazenar e processar dados de forma distribuída. Seu mecanismo de descentralização fornece soluções robustas para problemas de segurança e confiabilidade de sistema de informação, e tem sido utilizado no últimos anos para novas possibilidades para além das criptomoedas (Zheng et al., 2017).

A tecnologia de *Blockchain*, que encontra-se em pleno processo de desenvolvimento e utilização em diversos setores privados, também deverá influenciar as instituições públicas e suas formas de gestão (Momo et al., 2019). Este processo traz desafios à administração pública, em especial aqueles relacionados à apropriação desta tecnologias e ao estabelecimento de arranjos institucionais necessários à governança digital de processos baseados em *Blockchain*.

Assim, considerando a aplicação de tecnologias de *Blockchain* na administração pública, com especial destaque ao processo de identificação civil, evidencia-se que esta discussão ainda encontra-se em fase de amadurecimento técnico, científico e institucional no Estado brasileiro, conforme marco normativo relacionado. Há necessidade de evidenciar-se as possíveis aplicações e impactos da tecnologia de *Blockchain* no processo de identificação civil. A partir deste questionamento, este trabalho busca entender quais são as possíveis aplicações e consequências da utilização da *Blockchain* no processo identificação civil, na forma de uma Revisão Sistemática (RS) da literatura como procedimento metodológico voltado ao entendimento da problemática relacionada.

1.1 Contribuições desta Revisão Sistemática

Ao se considerar que o debate existente entre *Blockchain* e identificação civil pública encontra-se em fase de amadurecimento, esta RS busca responder as seguintes questões:

- Quais os possível impactos (positivos e negativos) que a tecnologia de *Blockchain* pode proporcionar ao processo de identificação civil público no território brasileiro?
- Quais as possíveis aplicações e consequências da utilização da *Blockchain* para a administração pública, com especial destaque para a garantia da segurança e privacidade dos dados envolvidos?

Embora alguns autores tenham realizado pesquisas no levantamento dos potencias uso de *Blockchain* no contexto da administração pública, no melhor de nosso conhecimento, há falta de trabalhos que forneçam uma discussão aprofundada no contexto de identificação civil. Desta forma, ao promover uma RS, as principais contribuições deste trabalho são:

i. Evidenciar *Blockchain* como uma potencial área de pesquisa, em pleno desenvolvimento, e suas oportunidades de aplicação em diferentes setores;
ii. Transpor uma nova experiência com identidades civis com validação eletrônica direcionando a importância de ter uma tecnologia que tenha suporte à evolução;
iii. Inovar com uma perspectiva de utilização da *Blockchain* para registros públicos mais eficientes e transparentes; e
iv. Trazer confiabilidade e qualidade na gerência dos dados governamentais, assim como celeridade nos processos da administração pública, contribuindo para inibir fraudes diversas e, principalmente, adulteração de documentos;

O restante deste trabalho está organizado da seguinte forma: A Seção 2 apresenta os principais conceitos relacionados a tecnologia de *Blockchain*, enquanto que a Seção 3 apresenta as etapas da RS e resultados obtidos, com uma análise crítica dos resultados. Por fim, a Seção 4 destaca os principais desafios e oportunidades de sistemas de identificação civil baseados em *Blockchain*, e a Seção 5 encerra este estudo, de forma a apresentar as considerações finais dos autores.

2 Blockchain

De acordo com a literatura relacionada, o conceito de *Blockchain* emergiu a partir da necessidade de se criar marcadores de tempo em documentos digitais, conforme seminal trabalho de Haber et al. (1991). Porém, o termo *Blockchain* surge a partir do trabalho de S. Nakamoto, como uma ferramenta para gerenciar criptomoedas, ao introduzir o *Bitcoin* como o primeiro sistema de moeda digital não-fiduciária P2P usando *Blockchain* (Nakamoto, 2008). Neste termos, a *Blockchain* cria um sistema de registro livro-razão (*ledger*) distribuído e completamente compartilhado, representando uma estrutura de dados que contém uma lista de transações de forma ordenada (conforme representado pela Fig. 1). Este livro-razão pode registrar transações realizadas entre várias contas *Bitcoin*, e após cada transação, as informações armazenadas no *ledger* são replicadas em todos os nós da *Blockchain* (Dinh et al., 2018). Desta forma, ao contrário dos bancos de dados tradicionais que possuem ambiente central, a tecnologia *Blockchain* funciona sobre um conjunto distribuído de nós, cada um possuindo informações sobre as transações que estão sendo realizadas em todos os nós da rede.

A partir das características mencionadas, observam-se características derivadas, como segurança no armazenamento dos registros, possibilitando a imutabilidade dos dados e aplicações e, desta forma, integridade e confiabilidade. E para completar a tríade CID, seu funcionamento descentralizado garante disponibilidade, além de fornecer uma rede de validação, de forma dificultar fraudes (Zachariadis et al., 2019). Porém, a utilidade da *ledger* baseia-se na concordância com seu conteúdo, dada a necessidade de eliminar a dependência de uma entidade centralizada. A *ledger* deve consolidar as transações efetuadas, de forma a viabilizar a cópia destas transações a todos os nós da rede. Por esse motivo, o acordo entre nós da rede, conhecido como consenso, é uma questão fundamental para a viabilidade da *Blockchain*, e um algoritmo de consenso específico deverá ser seguido por todos os nós da rede. Embora existam diversos algoritmos de consenso, Proof of Work (PoW) é a principal técnica que tem sido usada no *Bitcoin* e em diversas outras criptomoedas. Com o PoW, um quebra-cabeça matemático e criptográfico difícil é resolvido pelos mineradores para validar a transação e ganhar a recompensa. Algumas outras *Blockchains* adotam o algoritmo de Proof of Stake (PoS), onde uma abordagem pseudo-aleatória é utilizada para determinar o minerador. Neste algoritmo, as chances de mineração de um nó dependem da riqueza investida por esse nó específico na rede. Assim, quanto maior a riqueza de um nó, maior será sua chance de minerar o bloco e obter a recompensa (Saleh, 2020).

Ademais, redes *Blockchain* podem diferenciar-se em redes permissionadas e não-permissionadas. Em redes permissionadas, os nós são anônimos e sua entrada na rede é de livre acesso. Porém neste tipo de rede, os dados de transações são visíveis por todos os nós participantes. Por outro lado, as redes não permissionadas, seguem um modelo de funcionamento com nós participantes previamente selecionados, e, portanto, não anônimos. Porém, ganha-se a identificação dos participantes da rede junto com garantias criptográficas de privacidade das informações trafegadas nas redes, apenas entre os nós participan-

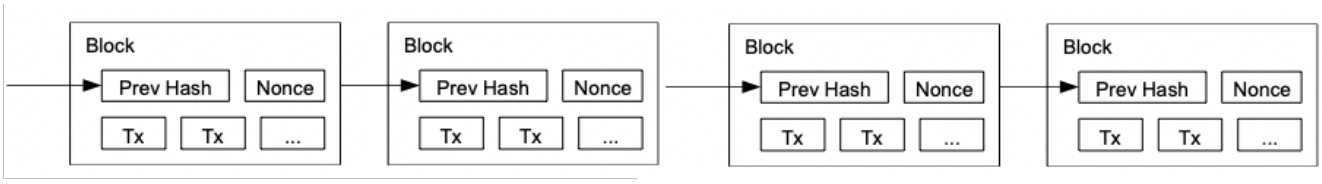

Figura 1: Representação do processo de encadeamento da *Blockchain*.

tes. Em ambos os casos, além de dados transacionais, há a possibilidade de armazenamento na *ledger* de aplicações (programas), conhecidos como contratos inteligentes - *Smart Contracts* (SCs). Com o uso de SCs é possível estabelecer negociações entre duas partes por meio de um *software*, prescindindo de intermediários centralizados. Neste termos, dada a imutabilidade proporcionada pela *ledger*, garante-se confiabilidade e integridade de funcionamento da aplicação. E, diferentemente de um contrato tradicional escrito em linguagem puramente jurídico-legal, um contrato inteligente é capaz de obter informações, executar rotinas, validá-las, processá-las e tomar as devidas ações previstas de acordo com as regras do contrato.

3 Revisão Sistemática

O estudo desenvolvido é de revisão sistemática. Esse método teve seleção pelo intuito do resumo de uma grande quantidade de informações que existe acerca de um fenômeno. Essas revisões podem permitir a incorporação de um espectro maior de resultados relevantes, ao invés da limitação das conclusões à leitura de apenas alguns artigos. Com isso, partindo da RS realizada, foi buscada a colaboração com o estudo de *Blockchain* e potenciais aplicações. Para a operacionalização dessa revisão, tiveram aplicação as principais premissas do método *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA), conforme definido por Galvão et al. (2015).

3.1 Etapas da RS

A sintetização das obras literárias em relação ao tema do trabalho, assim como para a contribuição para pesquisas futuras, tiveram adoção de aspectos com recomendação partindo do modelo PRISMA, principalmente os critérios de elegibilidade, análise e comunicação do estudo com aplicação às revisões sistemáticas. A RS teve seu início partindo da formulação da pergunta, seguida da localização das pesquisas detalhamento da busca. Em momento posterior, foi procedido para as avaliações críticas das pesquisas, criando filtros para a seleção dos estudos com relevância e posterior coleta de dados. Em finalização, foi realizada uma análise e apresentação dos dados, na extração de informações principais, para interpretar os dados e posterior análise crítica.

As perguntas-guias da RS foram: 'Quais os possível impactos (positivos e negativos) que a tecnologia de *Blockchain* pode proporcionar ao processo de identificação civil público no território brasileiro?' e 'Quais as possíveis aplicações e consequências da utilização da *Blockchain* para a administração pública, com especial destaque para a garantia da segurança e privacidade dos dados envolvidos?' Para que sejam respondidas essas perguntas, a estratégia de busca dos estudos valeu-se da definição da *string* de busca, com palavras-chave com capacidade de apresentar artigos que correspondiam à investigação. A Tabela 1 apresenta os resultados obtidos na primeira fase. De forma concomitante, à definição das *strings*, esta RS considerou os seguintes acervos literários, enquanto fontes de busca: *Web of Science*, *Scopus*, *Science Direct* e *IEEE Xplore*.

A partir da obtenção dos artigos, esta RS procedeu com a aplicação de filtros, exemplificado na Fig. 2, para selecionar artigos que trariam informações com relevância ao estudo. O primeiro filtro aplicado excluiu os trabalhos anteriores a 2017, uma vez que foi percebido que os estudos anteriores à data traziam informações mais conceituais sobre a tecnologia de *Blockchain*. O segundo filtro aplicado concentrou-se na escolha de artigos em língua inglesa e portuguesa, enquanto que o terceiro filtro foi baseado no tipo de produção literária. Em particular, esta RS concentrou-se em revisões sistemáticas, capítulos de livros, periódicos e trabalhos de conferência, desconsiderando-se, portanto, outras formas textuais. Em seguida, o quarto filtro aplicado baseou-se na análise dos resumos de cada trabalho, de modo que, utilizou-se como critério a identificação do termo *Blockchain* explícita em seu resumo, e terminologias que tivessem ligação com a identificação civil e a administração pública. Ao término dos filtros anteriores, restaram um total de 49 artigos, que foram submetidos ao quinto e último filtro, o de leitura completa e análise. Como resultado deste último filtro, restaram 21 trabalhos, que tem relação com o contexto de *Blockchain* para o processo de identificação civil, e a partir destes, fundamentam-se os principais achados desta RS.

3.2 Resultados Obtidos

Os resultados obtidos a partir da RS colaboram com a percepção de que, as pesquisas acerca da utilização de *Blockchain* relacionadas com identificação civil ainda são incipientes. No entanto, foi obtida uma conjuntura satisfatória das principais sugestões da aplicabilidade da *Blockchain*. A Fig. 3 apresenta os contextos de utilização da tecnologia *Blockchain* em diversos tipos de aplicação. Na subdivisão "processamento de dados" todos os artigos que tratam de governança e administração pública e os que utilizaram *smart contracts* fizeram uso da tecnologia *Blockchain*. Já na classificação "segurança de dados" os artigos que tratam de identidade auto-soberana e identidade digital em sua totalidade fizeram uso da tecnologia *Blockchain*, os outros artigos citam a tecnologia como em teste ou com potencial uso de desenvolvimento.

Os autores de Chen et al. (2019) relatam que as carac-

Tabela 1: *Strings* de busca e quantidade resultados obtidos para cada acervo.

#	Termo de Busca	Web of Science	IEEE Xplore	Scopus	Science Direct
1	blockchain AND identity AND management AND "public administration"	2	3	3	93
2	blockchain AND identity AND self-sovereign AND (NOT IoT) AND (NOT "smart city")	77	76	0	31
3	blockchain AND identity AND (ID OR SSN) AND (NOT IoT) AND (NOT "supply chain") AND contract	5	5	39	129
4	blockchain AND identity AND personnel AND ID	0	0	0	75
5	blockchain AND identification AND ID AND "identity management"	2	2	6	72
6	blockchain AND "personally identifiable information"	20	12	29	66

terísticas únicas da *Blockchain*, como não adulteração e rastreabilidade, fazem com que esta tenha um grande potencial de aplicação no gerenciamento de informações de pessoal, podendo resolver efetivamente diversos problemas relacionado ao gerenciamento tradicional de arquivos e dados pessoais.

O trabalho de Grüner et al. (2021) propõe que a *Self-Sovereign Identity* (SSI) seja uma identidade de aprimoramento de confiança para aumentar o potencial das SSI. O trabalho apresenta desafios consideráveis para uma adoção por provedores de serviço e consequente desenvolvimento de novos protocolos, enquanto Schlatt et al. (2021) demonstram como SSI baseada em *Blockchain* pode resolver os desafios de não violação dos dados de proteção e privacidade dos usuários. Assim para explorar a utilidade e a aplicabilidade de uma identidade auto-soberana - SSI, torna-se essencial esboçar alguns casos de uso da vida real. Tal processo ajudará a identificar alguns domínios de aplicativos essenciais ao qual o conceito de identidade auto-soberana trará vantagens significativas.

Em (Pennino et al., 2021), nas arquiteturas centralizadas as verificações geralmente são realizadas por autoridades de certificação confiáveis. Em aplicativos descentralizados, por exemplo, baseados em *Blockchains*, ou para gerenciamento de SSI, seria desejável realizar essas verificações de forma descentralizada, contando com o comportamento coletivo de uma sociedade de indivíduos ao invés de uma única entidade confiável.

No âmbito da saúde, diversos trabalhos tem sido conduzidos, como o trabalho de Hasan et al. (2020), que investiga uma solução baseada em *Blockchain*, que incorpora SSI, *proxies* de recriptografia e armazenamento descentralizado, como o *Interplanetary File System* (IPFS). A solução implementa passaportes médicos digitais e certificados de imunidade para os participantes do teste COVID-19. O trabalho sugere o uso de contratos inteligentes baseados em *Blockchain*, assim como em (Wang et al., 2019), trabalho desenvolvido com o objetivo de manter uma identidade médica digital para os participantes do teste que ajudam em uma resposta imediata e confiável diretamente pelas autoridades médicas relevantes, além de conter a propagação da doença através do passaporte médico digital.

O provedor de serviços e o usuário precisam confiar em um provedor de identidade específico para atributos corretos entre outras demandas. Esse paradigma mudou com a invenção da SSI baseada em *Blockchain* que traz soluções que se concentram principalmente nos usuários. O SSI reduz o escopo funcional do provedor de identidade para um provedor de atributos enquanto habilita a agregação de atributos. Além disso, o desenvolvimento de novos protocolos e desconsiderar os protocolos estabelecidos é um cenário significativamente fragmentado de soluções SSI que representam desafios para uma adoção pelos provedores de serviços, relatam Bernal Bernabe et al. (2019).

Conforme Gutiérrez-Agüero et al. (2021), o conceito de identidade tornou-se um tópico de pesquisa comum em segurança e privacidade onde a identidade real dos usuários deve ser preservada, geralmente coberta por identificadores pseudônimos. Com o advento de tecnologias *Blockchain*, as identidades estão se tornando ainda mais críticas, principalmente devido à propriedade de imutabilidade. De fato, muitas redes *Blockchain* acessíveis publicamente, como o *Ethereum*, contam com a pseudonimização como método de identificação das ações do sujeito. Pseudônimos são frequentemente empregados para manter anonimato, mas o verdadeiro anonimato requer não vinculação.

Segundo Shuaib et al. (2021), a principal motivação por trás da adoção de *Blockchain* em relação ao modelo cliente-servidor é fornecer confiabilidade, estabilidade, pontualidade e produtividade para o sistema, principalmente devido à sua descentralização. Hoje em dia, o mundo digital e o físico têm se tornado tão interconectados que a tecnologia de SSI é tão importante quanto a identidade física. O processo de autenticação e autorização para indivíduos e organizações é um fator recorrente importante em aplicativos *Blockchain*. A tecnologia atual não permite o processamento eficiente de informações digitais do usuário, mantendo a privacidade e a segurança deles. Nos modelos centralizados tradicionais, no âmbito da saúde, a privacidade dos pacientes é protegida por prestadores de serviços de saúde. Para obter acesso aos serviços, o paciente deve confiar no serviço dos provedores de saúde. Os modelos centralizados tradicionais têm muitas desvantagens, como dados perdidos devido a problemas relacionados aos dados de *hardware*. A tecnologia de SSI é baseada em um conjunto de princípios que precisam ser atendidos/realizados. Como tal, várias implementações são possíveis, mas no cenário atual, *Blockchain* é comumente usado para conceder aos indivíduos verdadeiro poder de administração sobre sua própria identidade, gerando assim modelos de acesso e propriedade de dados.

Moura et al. (2020) investigam como a tecnologia de *Blockchain* pode desempenhar um papel essencial na digitalização do setor público, não só em termos de *streaming* administrativo e consequente redução de custos e tempo, mas também porque permite uma melhoria significativa nos níveis de confiança, transparência, segurança, confiabilidade e acessibilidade dos serviços. No contexto de identificação civil, os autores indicam a possibilidade de confecção de documentos, como carteira de identidade, de trabalho, de habilitação, certidão de nascimento, de casamento, entre outros, que podem ter seu tempo reduzido com a *Blockchain*. Estes registros poderiam ser armazenados em um mesmo código, sendo de fácil acesso e confiável, tendo em vista a imutabilidade que a tecnologia oferece dos dados no sistema, corroborando com a perspectiva de

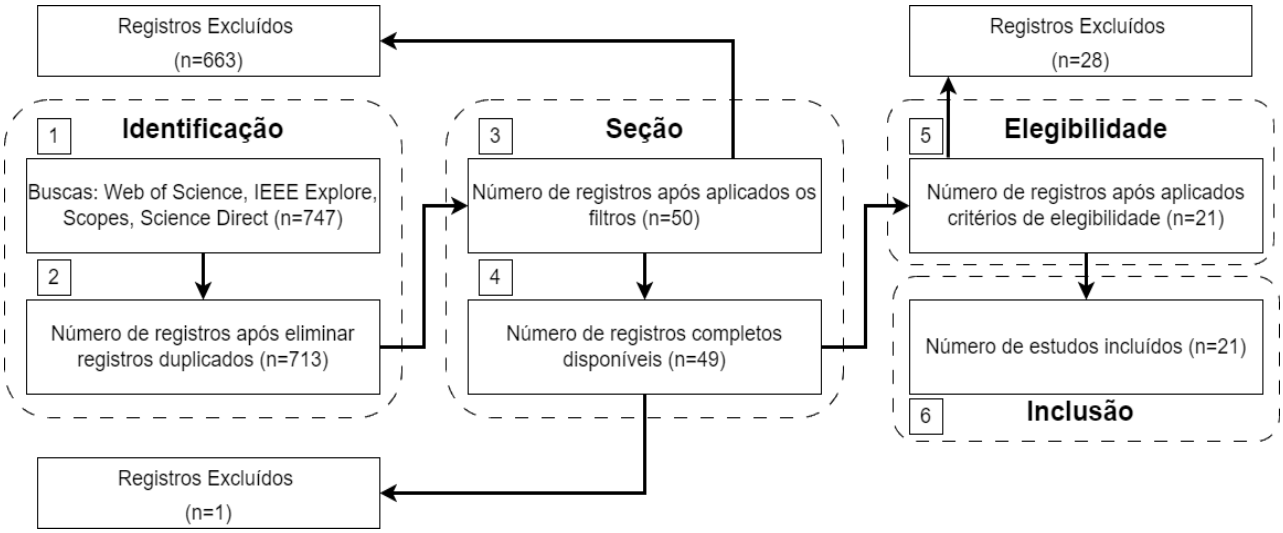

Figura 2: Sistematização dos filtros utilizados nos artigos selecionados.

registros públicos mais eficientes, transparentes, disponíveis e duráveis.

Em (Avgouleas and Kiayias, 2019) relata-se que *Blockchain* tem algumas características como: 1. O sistema não depende de organizações de gerenciamento centralizado ou *hardware* central; 2. Não há necessidade de confiar uns nos outros trocando dados entre os nós do sistema. Portanto, um nó não pode enganar outros nós; 3. Manutenção coletiva. Cada nó do sistema protege a segurança e a integridade do sistema de banco de dados completamente. 4. Resistência à violação. A menos que possa controlar mais de 51% dos nós, editar um único nó não afeta outros nós do banco de dados e não pode atingir o objetivo de adulteração de informações; 5. Rastreabilidade. Cada bloco de dados contém informações que podem ser rastreadas até a frente do conteúdo do bloco; 6. Anonimato. Os lados do nó podem ser negociados anonimamente e não precisam confiar um no outro; 7. Abertura, as informações da transação do nó são divulgadas e a transação entre os nós se torna transparente. O uso da tecnologia *Blockchain* sugerido no estudo, a partir de experimentos realizados para aumentar a fidelidade de plataformas/sistemas relevantes, tem um forte potencial de transformar tanto a estrutura em termos de redução de custos sociais quanto em relação aos benefícios da economia global, gerando estabilidade financeira.

Tan et al. (2022) indicam que a tecnologia de *Blockchain* é, de fato, adequada a contextos que exigem o compartilhamento seguro de dados intactos validados por terceiros. Segundo os autores, as soluções baseadas em *Blockchain* permitem a cooperação entre os cidadãos e as administrações públicas, otimizando e automatizando de forma segura os processos em conformidade com os requisitos de privacidade e confidencialidade, e ajudando a criar um ecossistema de eficiência e confiança entre os diferentes agentes envolvidos. Por outro lado, os autores sugerem que a adaptação de soluções automatizadas (baseadas em *Blockchain*) precisam estar em conformidade com as capacidades e práticas existentes no nível da sociedade em relação à governança digital. Isto é, há a necessidade de se avaliar até que ponto os cidadãos e governos podem gerenciar identidades e ativos digitais, o que pode inviabilizar, na visão dos autores, o conceito de SSI.

Por enquanto, em um momento em que os governos estão profundamente focados em custo-benefício e responsabilidade, e vêem esses aspectos como características-chave de uma boa formulação de políticas, as tecnologias que envolvam *Blockchain* precisam ser entendidas para organizar as soluções potenciais para uma série de desafios ou áreas de trabalho neste setor. Segundo os autores Silva and Marques (2021) é possível dizer que a tecnologia *Blockchain* tem potencial para permitir que o serviço público melhore a eficácia, reduza atritos entre agências, reduza barreiras burocráticas, melhore o compartilhamento de conhecimento e fomente a automação através de SCs.

Van Wingerde (2017) propõe um paradigma de identificação civil, baseado no conceito de SSI, viabilizado através da tecnologia de *Blockchain*. A proposta de um sistema descentralizado, para que o próprio sujeito possa gerenciar a administração de seus dados, apresenta-se como uma solução inspiradora. Para isso existem recursos atrativos da tecnologia, como ser descentralizada e distribuída, o que poderia ajudar a reduzir fraudes e cumprir as regulamentações existentes. No entanto, como sugerido, essa ainda não é uma solução viável para um sistema de gerenciamento nacional de identidade em um país que não é totalmente digital, mas pode ser o início de uma grande mudança para que se alcance a totalidade esperada neste gerenciamento.

Os autores Čučko and Turkanović (2021) e Stockburger et al. (2021) relatam que com o surgimento da tecnologia *Blockchain* e sua aplicação em diferentes domínios, a comunidade envolvida com identidades reconheceu seu potencial, pois os recursos do *Blockchain* coincidem com alguns propriedades da identidade digital. Assim, desde as primeiras discussões em 2015, o número de trabalhos de pesquisa abordando *Blockchain* e SSI aumentou, acumulando conhecimento e abrindo caminho para uma nova era de identidade digital. No entanto, o campo ainda é novo, desestruturado, nos estágios iniciais da pesquisa, com muitas oportunidades de pesquisa e desafios. Na maioria dos

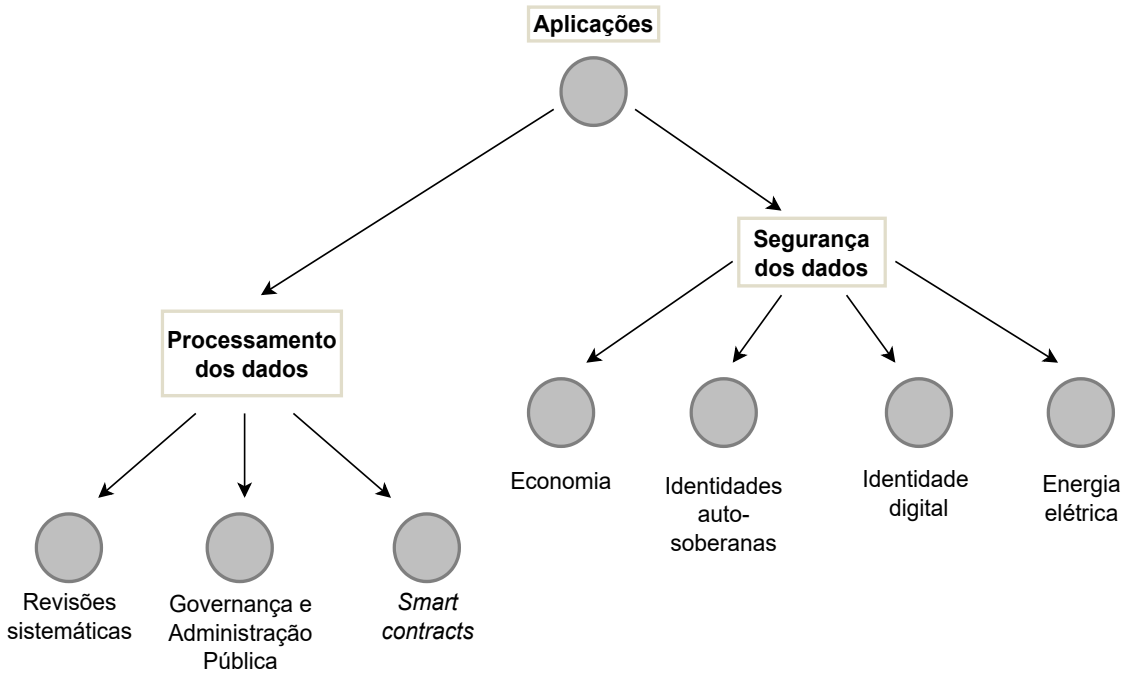

Figura 3: Sistematização do achados da RS, em termos de aplicações, perspectivas de utilização e casos de uso diversos da tecnologia de *Blockchain*.

casos, a pesquisa é realizada de forma geral (57,5%), não focando em um domínio específico. Apesar disso, o potencial em diversas áreas, como transportes, saúde, banca e governança, também é reconhecido.

Atualmente, com o advento da tecnologia *Blockchain*, existe um otimismo acerca do conceito de SSI que é considerado como tendo um efeito influenciador na forma como interagimos uns com os outros pela Internet no futuro. Apesar do exposto, os autores de (Ferdous et al., 2019) indicam que nenhuma das propostas de sistemas SSI satisfaz todas as propriedades necessárias que potencializam os conceitos associados ao SSI. Já os autores Houtan et al. (2020), ratificam essa questão, ao identificar que arquiteturas atuais baseadas em *Blockchain* e SSI ainda devem evoluir para melhor lidar com a privacidade dos dados envolvidos,principalmente em relação aos dados dos pacientes no âmbito da saúde.

Em (Seifert, 2020), autores relatam que o governo do Reino Unido anunciou que está procurando desenvolver identidades digitais seguras baseadas em SSI e *Blockchain* para os cidadãos. Um dos desafios destacado pelos autores baseia-se na necessidade de remover barreiras regulatórias que impedem o uso de identidades digitais seguras, de forma a estabelecer salvaguardas para os cidadãos. Uma das vantagens da adoção de SSI, segundo os autores, está no risco de a identidade de uma pessoa ou organização e informações de identificação serem roubadas por criminosos ser significativamente reduzido, pois estes não precisam mais entregar suas informações de identificação a milhares de bancos de dados.

Liu et al. (2020) sugerem que soluções de gerenciamento de identidade geralmente são projetadas para facilitar a manutenção de identidades digitais além de operações como autenticação e têm sido amplamente utilizadas em aplicativos do mundo atual. Alguns sistemas baseados em *Blockchain* podem ser descritos como uma revolução de identidade. Por exemplo, o sistema em que o usuário torna-se proprietário da identidade e não exigem que os usuários sacrifiquem a segurança pela conveniência.

O estudo conduzido por Sarier (2021) propôs um novo sistema baseado em *Blockchain* projetado para a indústria inteligente que permite auditoria adaptando o ciclo de vida de gerenciamento de identidade para *Internet of Things* (IoT) com custo computacional baixo, garantindo benefícios ao usuário.

4 Desafios e Oportunidades

A tecnologia *Blockchain* tem o potencial de catalisar grandes mudanças na prestação de serviços públicos e nas estratégias internas do governo como demonstrado pelos trabalhos (Moura et al., 2020) e (Tan et al., 2022), e em alguns casos, podendo resultar que as autoridades tradicionais não mais tenham o mesmo papel centralizador, mas passe a ser responsável por fornecer a legitimidade e a credibilidade para que essa nova tecnologia seja confiável.

A RS indica que a *Blockchain* não envolve apenas o setor financeiro, dada a crescente popularidade de criptomoedas, mas potencialmente subverte o funcionamento de toda a sociedade, representando uma verdadeira revolução da Internet. De acordo com Shen et al. (2022) esforços de pesquisa tem demonstrado o quanto a tecnologia de *Blockchain* é promissora, e suas características como descentralização, robustez e anti-modificação, representam

oportunidades, quanto um desafio significativo para o funcionamento, a regulamentação e a segurança de dados dos envolvidos.

A partir da condução desta RS, relacionam-se nas subseções a seguir, um conjunto de características que foram consideradas nos trabalhos selecionados na fase de inclusão. Estes trabalhos, em geral, tratam da criação ou reformulação de sistemas que atualmente estão em utilização nas mais variadas áreas da sociedade, e assim, sugere-se o aprimoramento destes sistemas, por meio da tecnologia de *Blockchain*. Consequentemente, a adoção da tecnologia de *Blockchain* tende a catalisar o aprimoramento ou a criação de novos sistemas com grande significância, em particular, dentro da Administração Pública.

Em resumo, a tecnologia de *Blockchain* possui pilares fundamentais que, potencialmente, trazem benefícios para o processo de criação de registros. Dentre estes pode-se citar:

- **Segurança da Informação:** A tecnologia de *Blockchain* pode contribuir com a garantia de princípio básicos de segurança da informação, como confidencialidade e integridade. Há diversos componentes de tecnologia subjacentes que ajudam neste processo, como funções de *hash* criptográfico, assinaturas digitais, criptografia de chave assimétrica, por exemplo;
- **Arquitetura Descentralizada:** Os registros de dados (blocos) não são armazenados em um servidor centralizado, sendo distribuídos entre os diversos nós partícipes da rede, de forma a garantir redundância e disponibilidade potencialmente global dos dados armazenados;
- **Protocolo de Consenso:** Para que uma nova transação seja inserida na rede, é necessário que um nó responsável deva verificar se essa transação é "verdadeira", e em caso positivo, a maioria desses nós (50% + 1) precisam 'aceitar' a sua inclusão. Este processo é implementado pelo protocolo de consenso, que é o principal componente utilizado para manter a consistência de uma *Blockchain*;
- **Imutabilidae:** A existência do encadeamento de cada bloco adicionado ao *hash* do bloco seguinte, faz com que a tentativa de modificação de um bloco seja virtualmente impossível dada a estrutura dos demais blocos. Ninguém pode alterar ou corromper uma transação na estrutura que é ordenada de forma cronológica. Sendo assim, nenhum dado novo pode ser apagado ou alterado de um bloco, o que garante um histórico temporal de tudo o que foi realizado.

4.1 Registros de Identificação na *Blockchain* (RIB)

A criação de Registros de Identificação na *Blockchain* (RIB) deverá trazer mudanças significativas para todos os âmbitos de identificação: civil, criminal e *pos-mortem*, pois garantirá segurança aperfeiçoada, além de gerenciamento de alto nível pelas partes envolvidas no processo de identificação civil. Com a adoção de RIBs, torna-se possível a criação de estrutura de armazenamento unificada e padronizada, que combinada com a característica de imutabilidade da *Blockchain*, pode garantir respostas imediatas e confiáveis transmitidas diretamente entre as autoridades e partícipes do processo de identificação civil, além de minimizar os riscos de fraudes.

Diferentes tipos de RIBs foram apresentados nos trabalhos analisados conforme Chen et al. (2019); Schlatt et al. (2021); Hasan et al. (2020); Wang et al. (2019); Bernal Bernabe et al. (2019); Shuaib et al. (2021); Moura et al. (2020); Avgouleas and Kiayias (2019); Silva and Marques (2021); Stockburger et al. (2021); Seifert (2020); Houtan et al. (2020); Liu et al. (2020); Sarier (2021). Embora os trabalhos apresentem-se em temáticas diferentes, todos consideram a adoção de RIBs em *Blockchains*, de tal forma que os sistemas de informação associados, se beneficiem das características inerentes da *Blockchain*.

4.2 Descentralização de Dados (DD)

Em trabalhos como (Pennino et al., 2021; Hasan et al., 2020; Avgouleas and Kiayias, 2019; Moura et al., 2020; Tan et al., 2022; Silva and Marques, 2021; Čučko and Turkanović, 2021; Stockburger et al., 2021), evidencia-se como aplicativos e sistemas podem se beneficiar da arquitetura P2P descentralizada oferecida pela *Blockchain*. Em geral, estes trabalhos apresentam protótipos de prova de conceito, prontamente escaláveis, aplicáveis genericamente e, com efeito, 'pronto para prosperar' em diversas áreas, além de abordarem questões éticas importantes.

Neste contexto, redes P2P são o mecanismo utilizado para disseminar as informações do sistema de forma resiliente, embora também, levantem novos desafios relacionados a sincronização e consenso dos nós participantes (Delgado-Segura et al., 2018). Ainda assim, o design descentralizado de sistemas P2P é utilizado para resolver o problema de conflitos existentes no modelo cliente/servidor,como por exemplo, quando o servidor falha as requisições dos clientes não podem ser atendidas, pois todos os nós da rede podem atuar tanto como cliente como quanto servidor.

Em um sistema de identificação civil esta característica seria de grande amplitude para estabelecer promissores níveis de confiança e conformidade. A descentralização tende a garantir a disponibilidade das informações, facilitando a identificação de possíveis falhas no sistema rapidamente, tornando-se assim um requisito fundamental para este tipo de sistema. Além disso, evidencia-se o aprimoramento da qualidade da informação, melhor tratamento dos dados além do maior e melhor monitoramento da coleta dos dados.

4.3 Uso de *Smart Contracts* (SC)

De acordo com Liu et al. (2020); Wang et al. (2019), os SCs podem encontrar um amplo espectro de possíveis cenários de aplicação na economia digital e indústrias inteligentes, incluindo serviços financeiros, gerenciamento, saúde, entre outros. Estes foram integrados à algumas das principais plataformas de desenvolvimento baseadas em *Blockchain*, como *Ethereum* e *Hyperledger*.

No caso da identificação civil, o uso de SCs é inovador e surpreendente, pois agrega potenciais oportunidades de aprimoramento no uso para sistemas que necessitem armazenar uma grande quantidade de dados. Uma vez que SCs são aplicativos (programas) registrados na estrutura

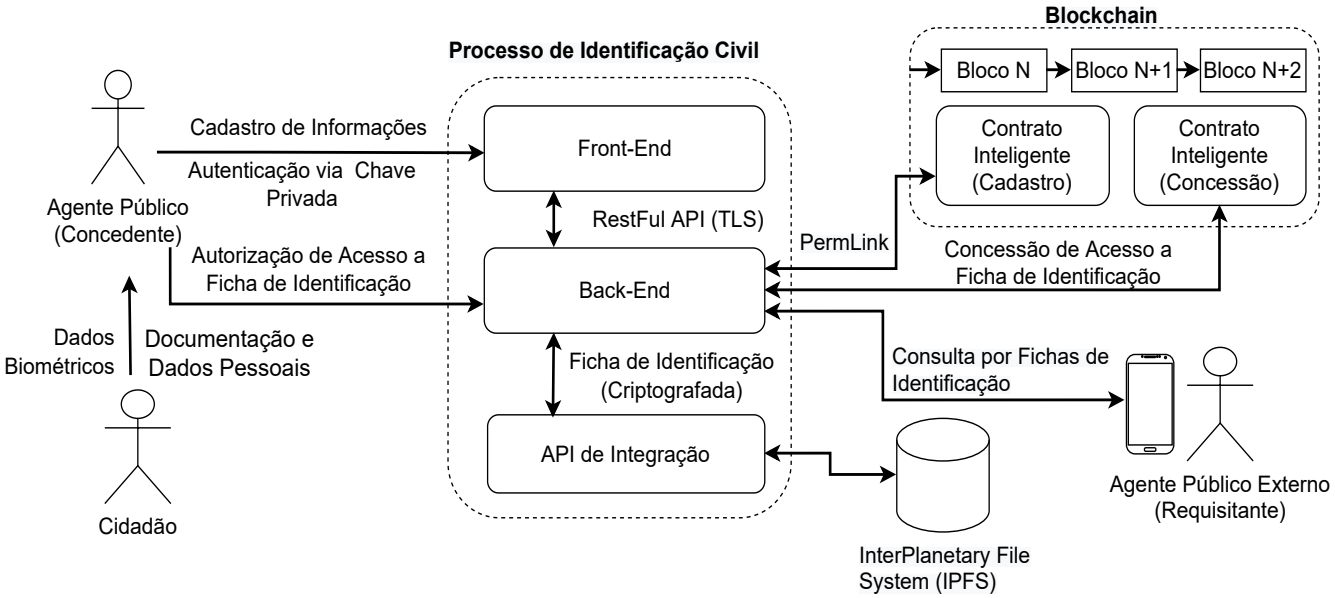

Figura 4: Representação de arquitetura visionada para processo de identificação civil com *Blockchain*.

da *Blockchain*, as funções de tais aplicativos são potencializadas pelos benefícios oferecidos pela *Blockchain*.

Desta forma, SCs podem ser utilizados, para automatizar procedimentos negociais de validação de uma identificação civil, ou ainda facilitar o processo de compartilhamento de informações entre as instâncias da segurança pública. Neste contexto, o uso de chaves criptográficas pode ampliar ainda mais a segurança do sistema, ao aprimorar a autenticidade e a confidencialidade dos dados armazenados na *Blockchain*. Com o uso de uma Infraestrutura de Chaves Públicas (ICP) torna-se possível a validação da expedição de documentos de identificação dos cidadãos, bem como a garantia de privacidade e confidencialidade destes dados. Desta forma, o processo de armazenamento desses documentos de identificação digitais executado por meio dos SCs garantirá, além do armazenamento seguro, alta disponibilidade e confiabilidade.

Adicionalmente, a imutabilidade proporcionada pela *Blockchain* garante integridade do código-fonte e dados manipulados por estes SCs. Embora haja a necessidade de quantificar a volumetria de dados inseridos na *Blockchain* por meio destes SCs (como por exemplo, na forma de *gas* na *Blockchain Ethereum*), a possibilidade de rodar uma aplicação de modo descentralizado e com garantias de disponibilidade e integridade, torna o serviço disponibilizado por tais SCs virtualmente a funcionar para sempre.

Este tipo de característica é bem vinda e oportuna a sistemas de identificação civil, dada a sua correlação com diversos processos da sociedade, como as identificações subsidiárias dela: criminais e *post mortem*, assim como a emissão de outros documentos advindos da identificação civil, que exigem agilidade e acesso sob demanda imediato as informações de identificação dos cidadãos.

Por outro lado, apesar de todas as possibilidade de aplicação dos SCs, a efetiva adoção ainda é emergente, mesmo nos trabalhos identificados por esta RS. Neste contexto, futuros estudos de adoção de de SCs podem contemplar a avaliação técnico-econômica de uso, onde custos operacionais associados podem ser avaliados, dada a necessidade de custeio do *gas*.

4.4 Contexto de SSI

SSI é uma abordagem de identidade descentralizada, emergente centrada no usuário, que utiliza alguma forma de tecnologia descentralizada (não necessariamente *Blockchain*). Esta fornece um meio para identificação digital sem depender de qualquer autoridade externa, permitindo que as entidades controlem sua identidade e fluxo de dados durante as interações digitais, enquanto aumenta a segurança e a privacidade destes dados. O termo 'identidade auto-soberana' é um dos termos de maior ocorrência nos trabalhos identificados por esta RS, bem como em particular nos trabalhos de Van Wingerde (2017); Ferdous et al. (2019); Houtan et al. (2020); Grüner et al. (2021).

Nos termos da legislação atual vigente, identidades civis são validadas através da emissão do documento físico, a carteira de identidade. Dessa forma, o Estado, na figura de responsável pela emissão das identidades, se perpetua como uma figura centralizada e historicamente considerada como confiável, que garante a identidade de cada cidadão.

Por outro lado, no mundo digital, ainda não existe uma forma fácil, segura e aceita pela maioria da população, capaz de provar quem são seus usuários no âmbito das identificações civis, criminais e *post mortem*. Ademais, a evolução da tecnologia SSI tenta resolver três problemas centrais da governança de dados: o primeiro é a segurança, uma vez que a informação precisa ser protegida contra possíveis fraudes e roubos de dados; o segundo é o controle, onde objetiva-se que o proprietário da identidade tenha gerência de quem pode ver e acessar seus dados e para quais fins; e o terceiro é garantir a portabilidade, que

Tabela 2: Principais características encontradas nos artigos.

#	Descentralização	Registro de Identificação *Blockchain*	Smart Contracts	SSI
Chen et al. (2019)	✓	✓	-	-
Grüner et al. (2021)	-	-	-	✓
Schlatt et al. (2021)	-	✓	-	✓
Pennino et al. (2021)	✓	-	-	-
Hasan et al. (2020)	✓	✓	-	-
Wang et al. (2019)	-	✓	✓	-
Bernal Bernabe et al. (2019)	-	✓	-	-
Gutiérrez-Agüero et al. (2021)	-	-	-	✓
Shuaib et al. (2021)	-	✓	-	✓
Moura et al. (2020)	✓	✓	-	-
Avgouleas and Kiayias (2019)	✓	✓	-	-
Tan et al. (2022)	✓	✓	-	-
Silva and Marques (2021)	✓	✓	-	-
Van Wingerde (2017)	-	-	-	✓
Čučko and Turkanović (2021)	✓	-	-	✓
Stockburger et al. (2021)	✓	✓	-	✓
Ferdous et al. (2019)	-	-	-	✓
Houtan et al. (2020)	-	✓	-	✓
Seifert (2020)	-	✓	-	✓
Liu et al. (2020)		✓	✓	✓
Sarier (2021)	-	✓	-	✓
Arquitetura Visionada	✓	✓	✓	✓

permitirá a utilização de dados onde o usuário quiser, sem vinculação a autoridade externa.

Os autores de (Schlatt et al., 2021; Gutiérrez-Agüero et al., 2021; Shuaib et al., 2021; Čučko and Turkanović, 2021; Stockburger et al., 2021; Seifert, 2020; Liu et al., 2020; Sarier, 2021) ponderam pela utilização de SSI em seus respectivos trabalhos de formas diversificadas, inclusive no contexto de saúde. Em todos os casos, as tecnologias de SSI e *Blockchain* são combinadas para potencializar os benefícios de ambas as tecnologias, em particular no que tange a garantia de privacidade e confidencialidade de dados dos usuários. No contexto de identificação civil, estas características podem ser utilizadas no momento atual da sociedade, para por exemplo, aumentar a segurança dos dados emitidos pela autoridades competentes. Uma abordagem baseada em SSI poderia promover um controle de autorização aprimorado, a quem poderia de fato acessar os (meta) dados de uma determinada pessoa.

4.5 Arquitetura Visionada

A partir dos trabalhos identificados nesta RS, a Fig. 4 apresenta a visão dos autores de uma proposta arquitetural, em como um sistema de identificação civil baseado em tecnologia *Blockchain* poderia ser concebido.

Inicialmente o cidadão repassará seus dados documentais e biométricos ao atendente inicial que filtrará a documentação necessária para a realização do processo de identificação civil. O atendente que possuirá uma autenticação com chave privada acessará o *Front-End* do sistema e cadastrará as informações fornecidas pelo cidadão. Este *Front-End* interage com o serviços disponibilizados pelo *Back-End* por meio de *RestFul API*, utilizando-se um túnel criptográfico com o protocolo *Transport Layer Security* (TLS), por exemplo.

O *Back-End* tem a função de consolidar os dados de identificação do cidadão, na forma de uma ficha de identificação civil, cujo formato digital poder ser em mídia *Non-Fungible Token* (NFT). Esta ficha de identificação pode ser armazenada em um repositório IPFS, por meio de uma API de integração. Para cada ficha de identificação consolidada no IPFS, um *permlink* (endereço) de identificação é gerado. Em seguinda, o *Back-End* tem a função de guardar esse *permlink* da *Blockchain*, via um SC dedicado a este processo de cadastro. Cabe ressaltar que, qualquer um com acesso a este *permlink* podederá acessar as fichas de identificação salvas no IPFS. Por este motivo, estas fichas são visionadas para serem criptografadas antes do processo de consolidação no IPFS.

A partir do cadastro, existe também a possibilidade desse documento gerado ser requisitado por outro órgão responsável ou autoridade competente. Inspirada nos paradigmas de SSI, quando o requisitante solicitar acesso para consultar algum dos documentos já cadastrados para verificação de dados será necessário que alguém conceda o acesso do mesmo por meio de um contrato inteligente de concessão já diretamente ligado à *Blockchain*. Neste processo de comunicação, intermediado pelo *Back-End*, deve-se contemplar um serviço de busca para as fichas de identificação por meio de um SC, além de um processo recuperação da ficha de identificação criptografada, e seu envio plano (decifrado) ao agente requisitante.

Em resumo, para que a ficha de identificação seja recuperada e encaminhada ao agente solicitante, existem dois processos que podem ocorrer:

i. Caso a resposta do agente público concedente para a obtenção da ficha de identificação negativa, já será o fim do processo. Nos termos de uma SSI, nenhuma ficha será recuperada, a não ser que haja a concessão da autoridade competente;

ii. Caso a resposta seja afirmativa, o *Back-End* confirma a autorização via SC, e recupera a partir desta o *permlink* associado. Em posse do *permlink*, o *Back-End* recupera a ficha de identificação e realiza sua decriptografia com as credenciais do agente concedente. Então, esta pode ser criptografada novamente, com a chave pública do agente solicitante, e enviada ao mesmo através do *Back-end* ao aplicativo deste agente.

Dessa forma a arquitetura visionada inspira-se nas características dos trabalhos identificados nesta RS (conforme ilustrado na Tabela 2), de forma a congregar tais características de forma a potencializá-las e contribuir com a modernização do processo de identificação civil no Brasil e no Mundo.

5 Considerações Finais

Apesar das possibilidade advindas da adoção da tecnologia de *Blockchain*, aplicações de curto e médio prazo no setor público devem ser singulares. Ainda é fundamental avançar em novos esforços de pesquisa que garantam que os recursos sejam manuseados com eficiência e segurança, e que as suposições e decisões subjacentes codificadas nas tecnologias *Blockchain* sejam compreendidas e obtenham o efeito desejado. Como potenciais impactos que a utilização da tecnologia *Blockchain* pode trazer no âmbitos das identificações civis, esta RS pode-se citar: transparência de dados, diminuição da burocracia, redução da corrupção, agilidade no processo e principalmente a melhoria no armazenamento e segurança dos dados. Nos processos de identificações civis, criminal e *pos-morten* muito ainda tem a ser feito, mas essa melhoria tecnológica tende a ser de grande relevância diante do cenário atual, e, principalmente, para de fato instituir o SIC, nos termos do Decreto 10.977 de 23 de fevereiro de 2022 (Presidência da República, 2022).

Agradecimentos

Este trabalho foi financiado em parte pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) e pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

Referências

Avgouleas, E. and Kiayias, A. (2019). The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment, *European Business Organization Law Review* **20**. https://doi.org/10.1007/s40804-019-00133-3.

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R. and Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges, *IEEE Access* **7**: 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872.

Chen, J., Lv, Z. and Song, H. (2019). Design of Personnel Big Data Management System based on Blockchain, *Future Generation Computer Systems* **101**: 1122–1129. https://doi.org/10.1016/j.future.2019.07.037.

Čučko, Š. and Turkanović, M. (2021). Decentralized and self-sovereign identity: Systematic mapping study, *IEEE Access* **9**: 139009–139027. https://doi.org/10.1109/ACCESS.2021.3117588.

Cui, W. and Zhang, N. (2017). Research and Development of Filing Management System of School Personnel Information based on Web, *Journal of Applied Science and Engineering Innovation* **4**(4): 127–130.

Delgado-Segura, S., Pérez-Solà, C., Herrera-Joancomartí, J., Navarro-Arribas, G. and Borrell, J. (2018). Cryptocurrency Networks: A New P2P Paradigm, *Mobile Information Systems* **2018**: 2159082. https://doi.org/10.1155/2018/2159082.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C. and Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems, *IEEE Transactions on Knowledge and Data Engineering* **30**(7): 1366–1385. https://doi.org/10.1109/TKDE.2017.2781227.

Ferdous, M. S., Chowdhury, F. and Alassafi, M. O. (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology, *IEEE Access* **7**: 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173.

Galvão, T. F., de Souza Andrade Pansani, T. and Harrad, D. (2015). Principais Itens para Relatar Revisões Sistemáticas e Meta-análises: A Recomendação PRISMA, *Epidemiologia e Serviços de Saúde* **24**: 335–342. https://doi.org/10.5123/S1679-49742015000200017.

Grüner, A., Mühle, A. and Meinel, C. (2021). ATIB: Design and Evaluation of an Architecture for Brokered Self-Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for Service Provider, *IEEE Access* **9**: 138553–138570. https://doi.org/10.1109/ACCESS.2021.3116095.

Gutiérrez-Agüero, I., Anguita, S., Larrucea, X., Gomez-Goiri, A. and Urquizu, B. (2021). Burnable Pseudo-Identity: A Non-Binding Anonymous Identity Method for Ethereum, *IEEE Access* **9**: 108912–108923. https://doi.org/10.1109/ACCESS.2021.3101302.

Haber, S. et al. (1991). How to time-stamp a digital document, *in* A. J. Menezes and S. A. Vanstone (eds), *Advances in Cryptology-CRYPTO' 90*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 437–455. https://doi.org/10.1007/BF00196791.

Hasan, H. R., Salah, K., Jayaraman, R., Arshad, J., Yaqoob, I., Omar, M. and Ellahham, S. (2020). Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates, *IEEE Access* **8**: 222093–222108. https://doi.org/10.1109/ACCESS.2020.3043350.

Houtan, B., Hafid, A. S. and Makrakis, D. (2020). A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare, *IEEE Access* **8**: 90478–90494. https://doi.org/10.1109/ACCESS.2020.2994090.

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K. and Raymond Choo, K.-K. (2020). Blockchain-based Identity Management Systems: A Review, *Journal of Network and Computer Applications* **166**: 102731. https://doi.org/10.1016/j.jnca.2020.102731.

Momo, F., Schiavi, G. S., Behr, A. and Lucena, P. (2019). Business Models and Blockchain: What Can Change?, *Revista de Administração Contemporânea* **23**: 228–248. https://doi.org/10.1590/1982-7849rac2019180086.

Moura, L., Brauner, D. F. and Janissek-Muniz, R. (2020). Blockchain e a Perspectiva Tecnológica para a Administração Pública: Uma Revisão Sistemática, *Revista de Administração Comtemporânea[online]* **24**(3): 259–274. http://doi.org/10.1590/1982-7849rac2020190171.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/en/bitcoin-paper.

Pennino, D., Pizzonia, M., Vitaletti, A. and Zecchini, M. (2021). Efficient Certification of Endpoint Control on Blockchain, *IEEE Access* **9**: 133309–133334. https://doi.org/10.1109/ACCESS.2021.3115343.

Presidência da República (2018). Lei nº 13.1709, de 14 de agosto de 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Presidência da República (2022). Decreto n. 10.977, de 23 de fevereiro de 2022. https://www.in.gov.br/en/web/dou/-/decreto-n-10.977-de-23-de-fevereiro-de-2022-382332304.

República Federativa do Brasil (1983). Lei n. 7.116, de 29 de agosto de 1983. http://www.planalto.gov.br/ccivil_03/leis/1980-1988/l7116.htm.

Saleh, F. (2020). Blockchain without Waste: Proof-of-Stake, *The Review of Financial Studies* **34**(3): 1156–1190. https://doi.org/10.1093/rfs/hhaa075.

Sarier, N. D. (2021). Efficient biometric-based identity management on the Blockchain for smart industrial applications, *Pervasive and Mobile Computing* **71**: 101322. https://doi.org/10.1016/j.pmcj.2020.101322.

Schlatt, V., Sedlmeir, J., Feulner, S. and Urbach, N. (2021). Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity, *Information & Management* p. 103553. https://doi.org/10.1016/j.im.2021.103553.

Seifert, R. (2020). Digital Identities Self-Sovereignty and Blockchain are the Keys to Success, *Network Security* **2020**(11): 17–19. https://doi.org/10.1016/S1353-4858(20)30131-8.

Shen, P., Li, S., Huang, M., Gao, H., Li, L., Li, J. and Lei, H. (2022). A Survey on Safety Regulation Technology of Blockchain Application and Blockchain Ecology, *2022 IEEE International Conference on Blockchain (Blockchain)*, pp. 494–499. https://doi.org/10.1109/Blockchain55522.2022.00076.

Shuaib, M., Alam, S., Shabbir Alam, M. and Shahnawaz Nasir, M. (2021). Self-Sovereign Identity for Healthcare using Blockchain, *Materials Today: Proceedings* . https://doi.org/10.1016/j.matpr.2021.03.083.

Silva, E. and Marques, R. M. (2021). Blockchain no Setor Público: Uma Revisão Sistemática de Literatura, *Revista AtoZ: Novas Práticas em Informação e Conhecimento]* **10**(3): 1–11. https://doi.org/10.5380/atoz.v10i3.79903.

Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016). Information Security Management needs more Holistic Approach: A Literature Review, *International Journal of Information Management* **36**(2): 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009.

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R. and Avital, M. (2021). Blockchain-Enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation, *Blockchain: Research and Applications* **2**(2): 100014. https://doi.org/10.1016/j.bcra.2021.100014.

Tan, E., Mahula, S. and Crompvoets, J. (2022). Blockchain Governance in The Public Sector: A Conceptual Framework for Public Management, *Government Information Quarterly* **39**(1): 101625. https://doi.org/10.1016/j.giq.2021.101625.

Van Wingerde, M. (2017). Blockchain-Enabled Self-Sovereign Identity: An Exploratory Study into The Concept Self-Sovereign Identity and How Blockchain Technology can Serve The Fundamental Basis. http://dx.doi.org/10.13140/RG.2.2.17693.82406.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X. and Wang, F.-Y. (2019). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends, *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **49**(11): 2266–2277. https://doi.org/10.1109/TSMC.2019.2895123.

Zachariadis, M., Hileman, G. and Scott, S. V. (2019). Governance and Control in Distributed Ledgers: Understanding the Challenges Facing Blockchain Technology in Financial Services, *Information and Organization* **29**(2): 105–117. https://doi.org/10.1016/j.infoandorg.2019.03.001.

Zheng, Z. et al. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85.