THIAGO YUKIO NAGATA ALVES

SISTEMA DE IDENTIFICAÇÃO DIGITAL BASEADO EM BLOCKCHAIN

São Paulo
2021

THIAGO YUKIO NAGATA ALVES

SISTEMA DE IDENTIFICAÇÃO DIGITAL BASEADO EM BLOCKCHAIN

Trabalho apresentado no Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos na Escola Politécnica da Universidade de São Paulo para obtenção do Título de Engenheiro.

São Paulo
2021

THIAGO YUKIO NAGATA ALVES

SISTEMA DE IDENTIFICAÇÃO DIGITAL BASEADO EM BLOCKCHAIN

Trabalho apresentado no Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos na Escola Politécnica da Universidade de São Paulo para obtenção do Título de Engenheiro.

Área de Concentração:

Engenharia Mecatrônica

Orientador:

Prof. Dr. Jun Okamoto Jr.

São Paulo
2021

AGRADECIMENTOS

Agradeço primeiramente a meus pais, a quem eu devo absolutamente tudo o que sou e que serei. Obrigado por priorizar a minha educação antes mesmo de eu nascer, apesar de todas as dificuldades financeiras. Espero conseguir retribuir a confiança, orgulho, amor e autonomia que vocês me presentearam por toda minha vida. O apoio e incentivo de vocês me permitiram focar exclusivamente na minha educação e foram cruciais para que eu pudesse chegar até aqui.

À minha namorada Maiara, quem colore a minha vida e me suportou incondicionalmente durante estes anos de imenso estresse. Obrigado por compreender os períodos de ausência e por contribuir pela leveza do meu ser.

Aos meus amigos, com quem eu compartilho momentos de felicidade e tristeza. Sei que independente de qualquer acontecimento, terei a fraternidade de vocês (x).

Aos profissionais de saúde que contribuíram direta ou indiretamente pela saúde física e mental da minha família e do Brasil.

A todos os professores da Poli por terem ensinado não apenas os conteúdos de engenharia, mas também o valor da autonomia.

Por fim, mas igualmente importante, agradeço ao meu orientador, professor Dr. Jun Okamoto Jr., que representa um exemplo de excelência e profissionalismo e a quem devo meus conhecimentos de programação e ética do trabalho.

RESUMO

A identificação de indivíduos possui ampla importância no contexto de administração pública, privada e individual. A identificação correta permite aos cidadãos utilizarem serviços que lhes são de direito em instituições públicas e privadas. Por outro lado, identificações falsas permitem a execução de crimes de fraude e tráfico. As falhas de identificação estudadas ocorrem pela incapacidade de um sistema autenticar um documento emitido por outro sistema. Sugere-se, portanto, que o problema decorre da falta de comunicação entre os sistemas de identificação existentes.

Foram estudados diferentes sistemas de identificação e analisados os padrões e tecnologias utilizados. Entre estes, destacou-se a estrutura de blockchain. Com o conhecimento dos sistemas existentes e utilizando metodologias de engenharia de *software*, foram levantados os requisitos para projetar um sistema que resolve o problema estudado.

O sistema de informação proposto é capaz de ser utilizado por múltiplas entidades compartilhando uma mesma base de dados para identificação civil. Esta característica garante que todas entidades do sistema possuam dados íntegros e autenticados, solucionando o problema apresentado.

ABSTRACT

Individual identification has great importance in the context of public, private and individual administration. Correct identification allows citizens to use services that are their right in public and private institutions. On the other hand, false identifications allow the occurrence of crimes of fraud and trafficking. The identification failures studied occur due to the inability of a system to authenticate a document issued by another system. It is therefore suggested that the problem arises from the lack of communication between the existing identification systems.

Different identification systems were studied and the standards and technologies used were analyzed. Among these, the blockchain structure stood out. With the knowledge of the existing systems and using software engineering methodologies, the requirements were raised to design a system that solves the studied problem.

The proposed information system is capable of being used by multiple entities sharing the same database for civil identification. This feature guarantees that all entities in the system have complete and authenticated data, solving the problem presented.

SUMÁRIO

1 INTRODUÇÃO

Um sistema de identificação certifica que um conjunto de dados únicos pertence a um indivíduo e possui suma importância no âmbito público, privado e individual. Os governos dependem das identificações pessoais para imigração, votações, coleta de impostos e distribuição de benefícios. Analogamente, empresas necessitam da identidade para a cobrança pelos produtos ou serviços oferecidos e análise de crédito. Além disso, é de interesse dos indivíduos que eles possam identificar-se para usufruir dos seus direitos e que nenhum outro possa fazê-lo.

O funcionamento de um sistema de identificação tem relevância tanto social quanto econômica e a sua falha causa prejuízos às partes envolvidas. Os custos de fraudes no ano de 2013, por exemplo, podem ter somado até R$ 10,11 bilhões apenas no setor privado brasileiro (Universidade de Brasília, 2014). Além disso, a falha de identificação é considerada fundamental para os crimes de terrorismo, tráfico de drogas, armas e pessoas (United Nations Office on Drugs and Crime, 2011).

Para a análise do problema, foram pesquisados diversos casos de crimes relacionados à falha de identificação. Verificou-se que uma das causas recorrentes dos crimes é a falta de comunicação entre os sistemas de identificação. Um dos exemplos eminentes é o da cédula de identidade brasileira. É possível um mesmo indivíduo emitir legalmente 27 identidades brasileiras com diferentes números e informações, visto que cada unidade federativa possui um sistema de identificação próprio.

Foram pesquisados diferentes tipos de métodos de identificação, que variam de país de origem, escopo de atuação, tecnologias utilizadas e instituições mantenedoras. O Governo Brasileiro, por exemplo, possui diversos sistemas independentes e tentou criar outros para unificá-los, mas com frequência não obteve sucesso. Uma das tentativas foi o Registro de Identidade Civil de 1997 (Presidência da República, 1997), que tinha como principal objetivo a unificação de documentos e o armazenamento da biometria, para garantir autenticidade. Os estudos técnicos do RIC foram suspensos em 2015 pelo Projeto de Lei nº 1.775, o qual propunha a implementação do sistema Registro Civil Nacional (RCN).

O RCN também visava a unificação de sistemas e a criação de um novo número de documento (CONGRESSO NACIONAL, 2015). Em 2017, o projeto foi transformado na Lei Ordinária n. 13.444, que deu origem ao Documento Nacional de Identidade (DNI) (Presidência da República, 2017).

A substituição total de um modelo para outro pode exigir uma mudança estrutural de tecnologia e processos, dificultando a implementação. Ademais, ao introduzir um novo número de documento, o sistema pode apenas adicionar mais complexidade ao problema. Cidadãos e instituições públicas e privadas teriam de continuar usando os documentos antigos até que a transição ao novo fosse realizada por completo.

Levando em consideração a necessidade de integração entre diferentes sistemas de identificação sem a criação de um novo documento, um sistema é proposto neste trabalho. O projeto garante que diferentes sistemas possam armazenar documentos já existentes utilizando o número de CPF de cidadãos como identificador único, dispensando a criação de um novo documento.

Fazendo uso da estrutura de blockchain no sistema proposto, múltiplas entidades compartilham a mesma base de dados e a autenticidade dos mesmos é garantida por assinaturas digitais. O compartilhamento permite que um sistema de identificação verifique a autenticidade de um documento, mesmo que tenha sido criado por outro sistema integrante da rede. Supõe-se que esta autenticação entre diferentes sistemas mitigaria a execução dos crimes estudados.

O projeto foi realizado utilizando metodologias de Engenharia de Software. Os requisitos de sistema foram traduzidos em casos de uso e foram feitos diagramas quando necessário. Modelou-se também a estrutura do banco de dados, bem como o protocolo de comunicação entre as entidades da rede blockchain.

Para testar a viabilidade do projeto, foi construído um protótipo. Este consistiu no desenvolvimento do servidor e de uma página *web* de cada participante do sistema. Foram realizados testes funcionais para averiguar a execução dos casos de uso. Os testes obtiveram sucesso e evidenciaram o cumprimento dos requisitos do projeto.

2 ANÁLISE DO PROBLEMA

O funcionamento de um sistema de identificação tem relevância tanto social quanto econômica e a sua falha causa prejuízos a todas as partes envolvidas, sejam elas entidades públicas ou privadas. A fraude nos sistemas de identificação são usados por criminosos para fuga da polícia, lavagem de dinheiro e desvio de benefícios de outros indivíduos. Os casos a seguir exemplificam a gravidade do problema.

Caso Pizzolato Houve um caso investigado em 2014, no qual o ex-diretor de marketing do Banco do Brasil, Henrique Pizzolato, emitiu um RG a partir da certidão de nascimento do seu irmão, Celso Pizzolato, falecido desde 1978. Pizzolato foi condenado pelo caso de corrupção apelidado de Mensalão em 2012, mas já havia expedido o RG falsificado em 2007, como parte do plano de fuga (MARTINS, 2014). Com o RG original em nome de seu irmão, Henrique conseguiu emitir um título eleitoral e o usou para votar nas eleições de 2008. A partir do título de eleitor e RG falsos, conseguiu também gerar um passaporte brasileiro verdadeiro. Em 2010, utilizou o seu conjunto de documentos para emitir um passaporte válido italiano.

A expedição de um RG de um cidadão falecido evidencia a ausência de validação de dados entre os sistemas da Secretaria de Segurança Pública, responsável pelo RG, e de Registro Civil das Pessoas Naturais, responsável pelo registro de óbitos. A mesma falha ocorreu nos sistemas do TSE, durante a criação do Título de Eleitor, e da Polícia Federal, na expedição do passaporte.

Caso Paulo Cupertino Em 2020, iniciou-se uma investigação sobre a emissão de um RG com dados falsos pelo homicida Paulo Cupertino. Em 2019, Cupertino estava foragido após matar a tiros uma família de três pessoas em São Paulo. Após o crime, Paulo viajou ao Paraná e requereu a emissão de um RG a partir de uma certidão de nascimento, CPF e um comprovante de residência falsificados. Nestes, o número de CPF, nome dos pais e o próprio nome de Paulo estavam adulterados. O RG foi criado normalmente e o criminoso o utilizou para receber dinheiro para pagar as suas despesas durante sua fuga (R7, 2020).

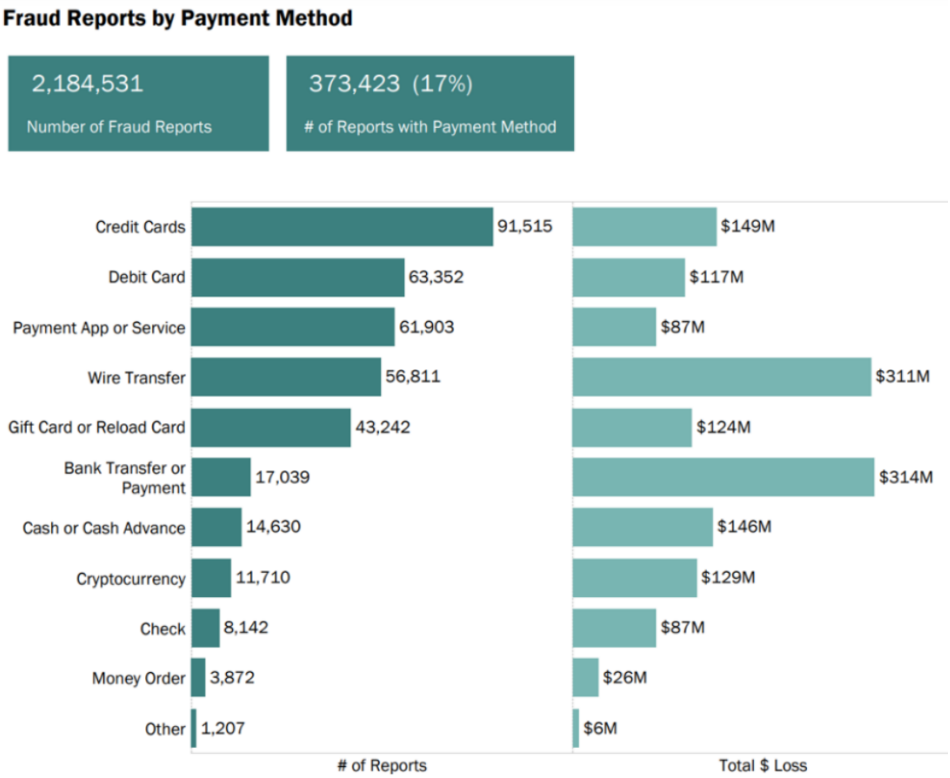
Neste caso, bastaria a verificação do número de CPF no sistema da Receita Federal para inibir a criação do documento falso, dado que o documento informado era inválido. Alternativamente, a certidão de nascimento também poderia ser verificada no sistema de Registro Civil. Como o nome do cidadão estava adulterado, bem como o de seus pais, a autenticação não seria aprovada.

Fraude nos benefícios do INSS Nos anos 2000 foi criado um grupo de investigação para averiguar fraudes nos benefícios do INSS, chamado Força Tarefa Previdenciária (FTP). Apenas em 2018, estima-se que a investigação preveniu o gasto de R$ 464 milhões em fraudes do INSS (TEIXEIRA, 2019). Entre 2014 e 2018, o valor estimado economizado pela prevenção chegou a R$ 1,3 bilhão (MAZZINI, 2019). Contudo, não é possível saber qual é o valor total das fraudes que ainda não foram descobertas. Em 2019, Marcelo Henrique de Ávila, coordenador geral da Inteligência Previdenciária brasileira, explicou que a investigação é feita a partir da consulta de múltiplas bases de dados públicas, como registro civil, título de eleitor, CPF, entre outros. Além disso, lamentou que não há um método seguro de identificação civil pelo poder público (TEIXEIRA, 2019).

O trabalho investigativo foi eficaz em evitar fraudes e consistiu em relacionar dados de diferentes sistemas de identificação. Entretanto, caso os próprios sistemas já possuíssem integração entre si durante a emissão de documentos e distribuição de benefícios, a investigação não seria necessária.

Fraude em pagamentos virtuais A consultoria Juniper Research estima que houve uma perda global de US$ 27 bilhões em fraudes de pagamento online em 2020 e esse número pode chegar a US$ 52 bilhões em 2025 (MAYNARD; MORROW, 2021). A figura 1 expõe os valores perdidos em fraudes relatadas no ano de 2020.

Figura 1: Casos de fraude relatados em 2020



Fonte: Extraído de (MAYNARD; MORROW, 2021)

Segundo a Serasa Experian, empresa especializada no mercado de crédito, a fraude mais comum de 2017 foi a abertura de contas de telefone com dados alheios. Os fraudadores enviam documentos alegando ser a vítima do golpe, mas com um endereço diferente do real. Com a conta criada, os criminosos obtêm um comprovante de residência e um número de telefone válidos. Estes recursos são suficientes para abrir contas em outras instituições, como bancos, cooperativas de crédito e lojas virtuais. Em seguida, emitem cartões de crédito, contraem empréstimos ou fazem compras em nome da vítima. Assim, os fraudadores adquirem o dinheiro, enquanto a responsabilidade recai sobre os titulares (EXPERIAN, 2021).

As fraudes financeiras resultantes da criação de contas com documentos falsos poderiam ser evitadas com a verificação de autenticidade das informações nos sistemas de identificação públicos. Uma listagem pública poderia ser considerada invasão de privacidade, pois informaria o número do telefone e endereço do cidadão, por exemplo, para uma empresa privada que não possui tal informação. Entretanto, caso a empresa recebesse os dados do próprio cidadão, poderia consultar a veracidade dos mesmos sem quebra de privacidade.

Síntese do problema Todos os casos apresentados poderiam ser evitados pela verificação da autenticidade dos documentos fornecidos pelos criminosos. Entretanto, não há um serviço público centralizado que permita a validação de todos os tipos de documentos. Cada sistema público de identificação possui responsabilidade por um documento diferente, dificultando a integração entre os mesmos. Em suma, o problema é solucionado por um sistema caso os requisitos sejam cumpridos:

- Documentos de identificação de diferentes emissores são armazenados no sistema;
- A autenticidade de cada documento é garantida pelo seu emissor;
- Qualquer sistema público ou privado pode consultar a autenticidade de um documento fornecido, independente do emissor do mesmo.

No próximo capítulo foram estudados diversos sistemas de identificação existentes para compreender as práticas utilizadas e avaliar o cumprimento dos requisitos levantados.

3 SISTEMAS DE IDENTIFICAÇÃO DIGITAL

Existe uma grande variedade de soluções para o problema de identificação civil. Estas, que geralmente são criadas por empresas ou governos, diferem em seus métodos de verificação de autenticidade, mantenedores do sistema e tecnologias envolvidas. Foram estudados sistemas de identificação utilizados em diferentes países, bem como soluções privadas.

3.1 Identificação no Brasil

Os primeiros sistemas de identificação brasileiros tinham um objetivo específico, como a identificação de um eleitor, condutor ou imigrante. Assim, geralmente criavam novos documentos diferentes, como o título de eleitor e a carteira nacional de habilitação. Por outro lado, desde o projeto RIC de 1997, o foco dos novos sistemas passou a ser o agrupamento de documentos anteriores.

Tabela 1: Sistemas de identificação brasileiros

Documento/Sistema	Ano
Título eleitoral	1875
Passaporte brasileiro	1891
Cadastro de Pessoas Físicas (CPF)	1965
Carteira Nacional de Habilitação (CNH)	1981
Registro Geral (RG)	1983
Registro de Identidade Civil (RIC)	1997
Documento Nacional de Identificação (DNI)	2017
Cadastro Base do Cidadão (CBC)	2019

Atualmente, cada documento possui um órgão responsável por auferir a autenticidade dos dados e emitir o documento. Para expedir documentos, sempre é necessário que o cidadão apresente um documento prévio. A vulnerabilidade no sistema ocorre quando o órgão não possui os meios de autenticar o documento fornecido pelo cidadão.

A multiplicidade de documentos também traz inconveniências para os cidadãos. Um cidadão interessado na emissão de passaporte, por exemplo, deve apresentar o RG ou a CNH, desde que acompanhada com outro documento que comprove o local de nascimento. Estes documentos são expedidos pela Secretaria de Segurança Pública, DETRAN e Registro Civil, respectivamente. Para renovar seus documentos, o indivíduo é obrigado a ir a diferentes órgãos públicos. A tabela a seguir resume as informações disponíveis em cada tipo de documento:

Tabela 2: Comparação de documentos e sistemas

	Título eleitoral	Passaporte	CPF	RG	CNH	RIC	DNI	SIRC	CBC
Órgão responsável	TSE	Polícia Federal	Receita Federal	Governo estadual	DENATRAN	Minist. da Justiça	TSE	INSS	CCGD
Nome	✓	✓	✓	✓	✓	✓	✓	✓	✓
N. CPF	✓		✓	✓	✓	✓	✓	✓	✓
N. RG	✓				✓	✓	✓	✓	
N. CNH	✓				✓	✓	✓		
N. Título eleitoral	✓					✓	✓		✓
Data de nascimento	✓	✓	✓	✓	✓	✓	✓	✓	✓
Biometria	✓			✓		✓	✓		✓
Fotografia	✓	✓		✓	✓	✓	✓		✓
Filiação			✓	✓	✓	✓	✓		✓
Sexo		✓	✓			✓			✓
Data de óbito								✓	✓
Assinatura	✓	✓		✓	✓	✓	✓		
Tipo sanguíneo							✓		
Estado civil							✓	✓	

3.1.1 Prova de conceito com blockchain

O Ministério do Planejamento do Governo Brasileiro realizou uma prova de conceito de um sistema de identificação digital baseada em blockchain em 2017. O projeto envolveu a parceria do Ministério com a Microsoft e a ConsenSys, criadora da uPort. Estudou-se nesta iniciativa a integração dos serviços públicos com o serviço de identificação com blockchain (ETHNEWS, 2017).

Segundo Adriane Medeiros Melo, chefe do Departamento de Tecnologia da Informação do Ministério do Planejamento, a tecnologia de blockchain promove auditabilidade e segurança de informação na internet, por ser distribuído e não possuir um único ponto de falha. Além disso, alega que promove uma diminuição do tempo e custo das operações relacionadas a identidades digitais (International Business Times, 2017). Não houve

anúncios de continuação do projeto após a prova de conceito.

3.2 Identidade digital na Alemanha

Na Alemanha, não há um documento unificado de identificação civil, porém é obrigatório que maiores de 16 anos possuam uma identidade ou passaporte. Os documentos comportam nome, data e local de nascimento, foto, altura, cor dos olhos entre outros. Em ambos documentos, existe um chip de rádio frequência (RFID) que salva parte dos dados impressos em sua memória (Federal Office for Information Security of Germany, 2010).

A criação dos documentos é de responsabilidade das emissoras públicas, porém estas não armazenam os dados dos usuários. Como as informações são consultadas sempre pelo documento, considera-se que o modelo alemão é centrado no usuário.

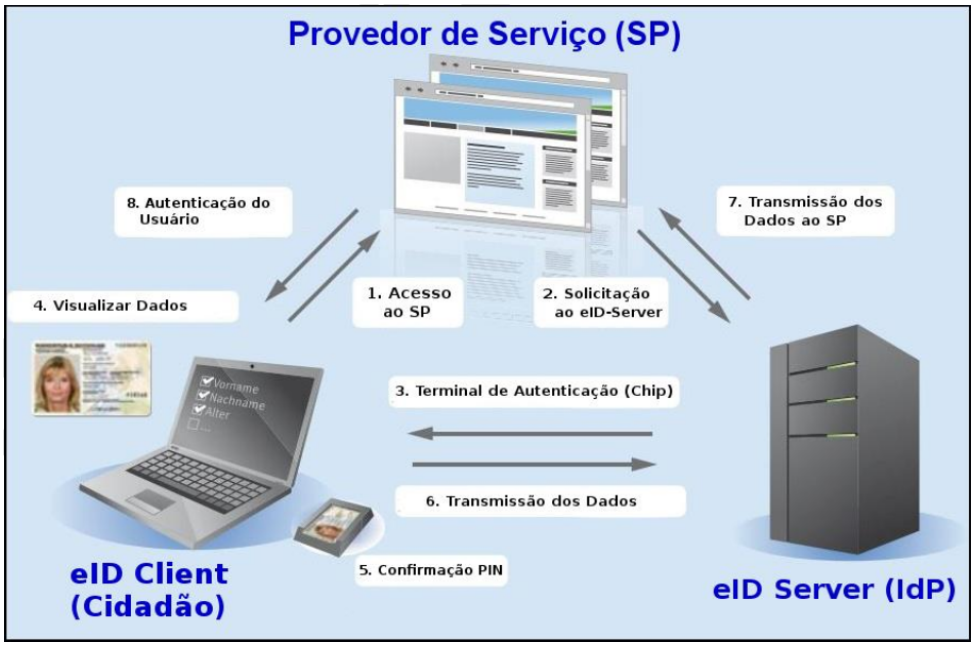
Os dados do microchip são assinados com um certificado Country Signing Certificate Authority (CSCA), garantindo a integridade dos dados. Esta assinatura digital é também salva no RFID e sua criação é limitada apenas para os fabricantes autorizados dos cartões.

O sistema descentralizado de identificação alemão segue a especificação SAML. O protocolo SAML (*Security Assertion Markup Language*) é um padrão para a criação sistemas de identificação criado pela OASIS (*Organization for the Advancement of Structured Information Standards*). Sua versão atual é a 2.0, que foi efetivada como padrão pela Organização em 2005. A especificação define tanto a estrutura de entidades participantes do sistema quanto o protocolo de comunicação em XML a ser utilizado por elas (HUGHES et al., 2005).

O SAML define três atores no sistema: usuário, provedor de serviço e provedor de identidade. O usuário inicia o processo de autenticação com uma requisição ao provedor de serviço, com seus dados de acesso. O provedor de serviço consulta o provedor de identidade para a autenticação e posteriormente pode conceder uma credencial de acesso ao usuário. O método de autenticação das informações pelo provedor de identidade encontra-se fora de escopo do protocolo e é específico de cada implementação.

No caso da Alemanha, os provedores podem ser públicos ou privados e devem ser homologados pelos Ministério Federal do Interior (IMC) e Departamento Federal de Segurança em Tecnologia da Informação (BSI). Os dados estão sempre em posse do usuário civil, de modo que os provedores de identidade não possuem os dados em si, agindo apenas como intermediador entre o cliente e o provedor de serviço.

Figura 2: Processo de autenticação do sistema alemão



Fonte: Extraído de (Universidade de Brasília, 2015)

O cliente entra em um Provedor de Serviço (SP), que por sua vez requisita determinados dados do usuário para um Provedor de Identidade (IdP). O IdP verifica a autenticidade de ambas entidades por seus certificados e aguarda a confirmação por PIN do usuário. Uma vez que o usuário escolhe os dados permitidos para o provedor de serviço, estes são enviados para o provedor de identidade. O IdP por sua vez retransmite os dados ao SP, finalizando a autenticação do usuário.

3.3 Identidade digital na Itália

Na Itália, foi criado o projeto da criação de um documento de identidade eletrônico em 2001. O seu uso não é obrigatório e nele são contidos um conjunto de dados básicos, tipo sanguíneo e impressão digital do cidadão. A sua emissão é feita por uma das quase 8 mil comunas italianas, ou seja, o sistema segue um modelo distribuído de criação e autenticidade do documento (DELL'INTERNO, 2001).

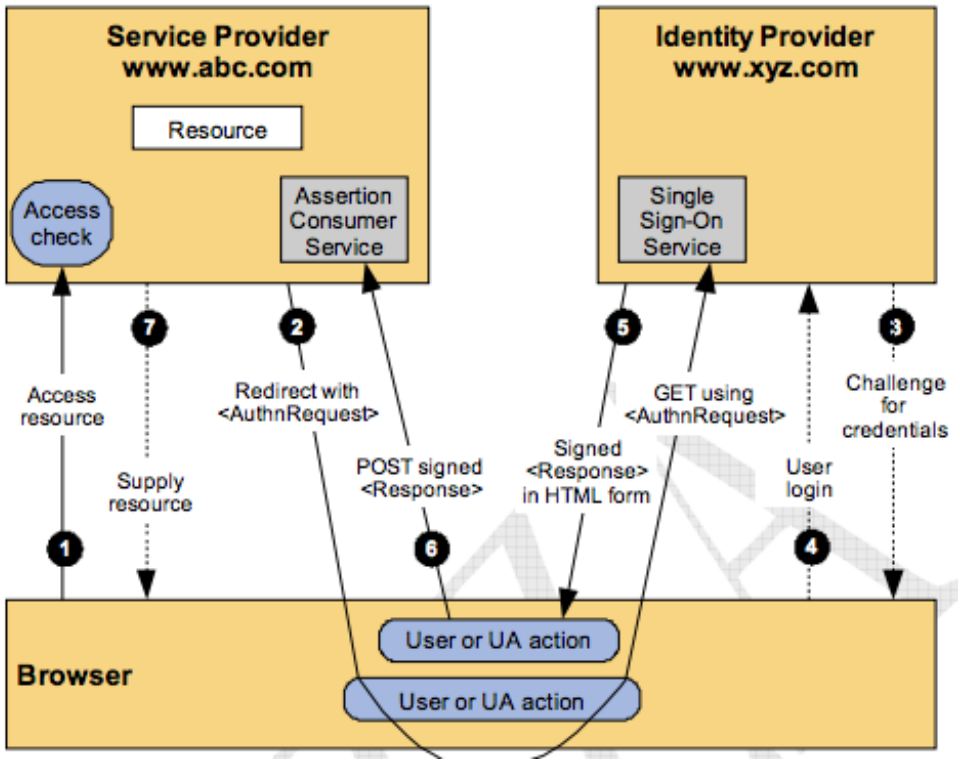
Por motivos de segurança, os dados do cartão, juntamente com a chave biométrica e o certificado digital, são armazenados apenas no microchip do cartão (European Comission, 2016). Isto significa que, assim como o modelo alemão, o sistema de armazenamento de dados é centrado no usuário.

Para a integração com serviços públicos, em 2015 foi lançado um sistema de identifi-

cação chamado Sistema Pubblico di Identità Digitale (SPID) que segue os padrões SAML 2.0. Entretanto, diferentemente da arquitetura alemã, os provedores de identidade são controlados apenas por entidades públicas (Agenzia per l'Italia Digitale, 2014).

Foram emitidas mais de 2,5 milhões de identidades no sistema SPID, com crescimento anual de 171%. Com o sistema, é possível um cidadão utilizar serviços públicos de todos os países da União Europeia. Apesar de atualmente os provedores de identidade serem limitados à iniciativa pública, há um planejamento para a abertura do serviço a entidades privadas (Italian Digital Transform Team, 2018).

Figura 3: Ilustração da autenticação no sistema SPID



Fonte: Extraído de (Agenzia per l'Italia Digitale, 2014)

3.4 Identidade digital na Estônia

Na Estônia, todos os cidadãos recebem um número de registro civil único no nascimento. Este registro é utilizado para criar um documento de identidade chamado ID Card (ESTONIA, 2018). A identidade é considerada obrigatória para cidadãos maiores de 15 anos e para qualquer residente estrangeiro.

O cartão possui um chip eletrônico, que pode ser usado para assinar documentos digitalmente, usar serviços de autenticação e até para votação online. Alternativamente,

existe a possibilidade de o cidadão utilizar o cartão apenas como identidade física. Os serviços de identificação online tem como método alternativo o chamado Mobile ID, que consiste em gravar os certificados digitais no cartão SIM do celular, para utilizar as funções com o mesmo valor legal.

O ID Card possui dois certificados digitais: um para autenticação e outro para assinaturas digitais. Ambos certificados são emitidos pela autoridade de certificação chamada AS Sertifitseerimiskeskus (SK), única do país. O sistema centralizado foi projetado pelo Governo estoniano e é controlado pela Polícia Especial da Estônia. O sistema de identificação pode ser usado tanto em sistemas públicos quanto privados, porém as verificações de autenticidade são realizadas sempre pela empresa SK, sob supervisão estatal.

3.5 Plataforma Civic

A plataforma Civic consiste em uma iniciativa privada que tem como objetivo a autenticação de dados individuais para empresas prestadoras de serviços (Civic Technologies, 2017). Os usuários da plataforma devem baixar o aplicativo e cadastrar os dados em seu perfil, simulando uma identidade virtual.

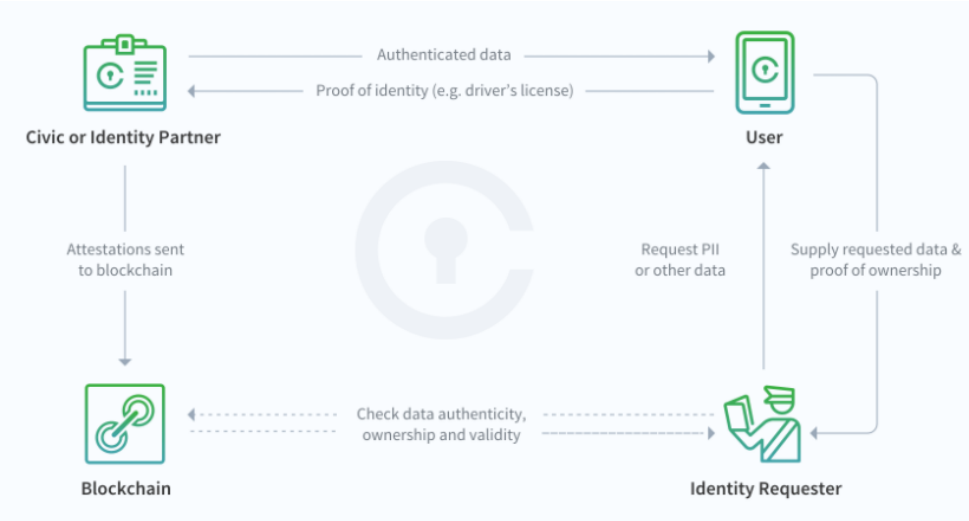
Estes dados são então encriptados localmente e somente acessíveis após uma validação biométrica do usuário, como reconhecimento facial ou por impressão digital. Para garantir a integridade dos dados, assinaturas digitais são geradas e enviadas ao servidor do sistema. As assinaturas são então salvas no sistema Ethereum, cuja estrutura de dados é chamada de blockchain. Será explicado posteriormente como os dados inseridos nesta estrutura de dados são imutáveis.

Para que uma instituição utilize os serviços da plataforma, a mesma deve ser contratante da Civic, assim como os clientes a serem identificados. No caso deste sistema de identificação, a verificação de integridade e de autenticidade dos dados se dão em momentos distintos, ambos após a aprovação biométrica do usuário. A verificação de integridade ocorre com a recriação da assinatura digital dos dados recebidos do usuário e na sua consulta na rede blockchain. Uma vez verificada, a plataforma segue para a autenticação dos dados, baseando-se em terceiros, como instituições financeiras e governos.

Finalmente, a empresa interessada recebe os dados do usuário com garantia de integridade pela plataforma Civic e de autenticidade por uma instituição terceira. Paralelamente, a autenticação dos dados é salva pela plataforma na blockchain, para futuras consultas. Dessa maneira, existe a garantia imutável de integridade dos dados e uma

crescente confiança de autenticidade dos dados, gerada por instituições externas.

Figura 4: Processo de identificação do sistema Civic



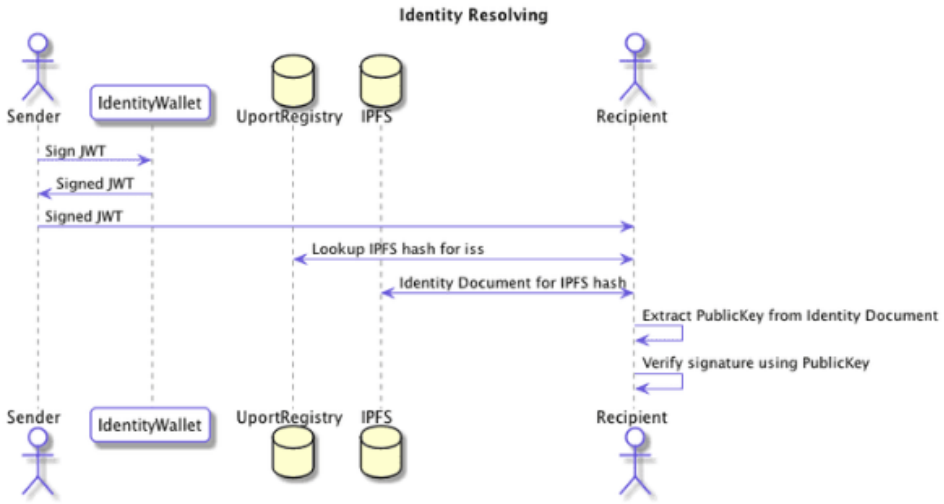
Fonte: Extraído de (Civic Technologies, 2017)

3.6 Plataforma uPort

A uPort é uma plataforma de identificação centrada nos usuários, de modo que estes tenham controle total sobre suas informações (UPORT, 2018). A empresa é responsável pela criação de recursos para provedores de serviços e consumidores. Para os usuários, a uPort oferece um aplicativo para o gerenciamento de dados, credenciais e acessos concedidos a empresas. Para provedores de serviços, cria protocolos e ferramentas para a integração com a plataforma.

Na uPort, os usuários conseguem salvar informações pessoais, conceder acesso a terceiros e criar assinaturas digitais. A validação direta da autenticidade dos dados dos usuários se encontra fora de escopo dos serviços oferecidos pela plataforma. Os dados, como nome e endereço, são denominados "alegações", pela ausência da confirmação de autenticidade. De maneira semelhante à plataforma Civic, terceiros podem criar e apoiar alegações de usuários, atribuindo mais confiança a elas (BRAENDGAARD; UPORT, 2018). Assim como a Civic, a uPort é desenvolvida sobre a plataforma Ethereum, que utiliza a estrutura de dados de blockchain. Para comunicação *off-chain*, com os usuários e provedores de serviço, a empresa utiliza JSON Web Tokens (JWT), de acordo com o padrão RFC 7519 (JONES et al., 2015). Este tipo de *token* pode ser utilizado como credencial entre provedores de serviço e identidade, analogamente ao padrão SAML.

Figura 5: Diagrama de sequência de uma identificação na plataforma uPort



Fonte: Extraído de (UPORT, 2018)

Para o armazenamento de dados, a empresa uPort optou pelo uso do protocolo IPFS. O protocolo cria um único sistema de arquivos de maneira distribuída entre uma rede de computadores. O IPFS tem como vantagem a imutabilidade de dados e a inexistência de um ponto único de falha (BENET, 2017). O armazenamento de informações pessoais na plataforma é de escolha dos usuários (BRAENDGAARD; UPORT, 2018). No início de 2021, a plataforma uPort foi descontinuada. A empresa passou por uma reestruturação de modelo de negócios, time e tecnologias, passando a se chamar Serto (UPORT, 2021).

3.7 Comparação

Com o estudo de diferentes sistemas de identificação, evidenciam-se contrastes estruturais. Entre estes, diferenciam-se a estrutura de garantia de autenticidade, dos provedores de identidade e do armazenamento de dados. Nota-se também que os sistemas privados foram desenvolvidos sobre uma plataforma já existente, diferentemente dos sistemas governamentais.

As plataformas Civic e uPort, possuem um gasto operacional por serem desenvolvidas como aplicações no Ethereum Blockchain. Para a execução dos seus programas e armazenamento de dados, as plataformas pagam aos sustentadores da rede. Além disso, o desenvolvimento sobre uma blockchain pública resulta em um problema de segurança de dados. Apesar de os dados serem encriptados, as informações transacionadas nestes tipos de rede são públicas, por definição.

Tabela 3: Comparação dos sistemas de identificação

Sistema	Governo Alemão	Governo Estoniano	Governo Italiano	Plataforma Civic	Plataforma uPort	Proposta
Iniciativa	Pública	Pública	Pública	Privada	Privada	-
Garantia de autenticidade	Distribuída Pública	Centralizada Pública	Distribuída Pública	Distribuída Pública ou Privada	Distribuída Pública ou Privada	Distribuída Pública
Estrutura do sistema	Distribuída	Centralizada	Distribuída	Distribuída	Distribuída	Distribuída
Participação do sistema	Controlada	Livre	Livre	Controlada	Controlada	Controlada
Armazenamento dos dados	Centralizado no usuário	Centralizado no sistema	Centralizado no usuário	Centralizado no usuário	Centralizado ou Distribuído no usuário ou sistema	Centralizado no sistema
Especificações	SAML	-	SAML	Ethereum Blockchain	Ethereum, JWT	-

O sistema proposto neste trabalho se baseia nas estruturas dos sistemas de identificação estudados e utiliza conceitos de cada um deles. Escolheu-se o desenvolvimento de uma rede blockchain própria e controlada para evitar custos operacionais inerentes das redes públicas e garantir o acesso aos dados apenas às entidades permitidas. O modelo proposto tem como objetivo a integração dos sistemas de identificação brasileiros existentes, mas não sua substituição. Por este motivo, a garantia de autenticidade dos documentos ainda fica de responsabilidade dos órgãos públicos. Portanto, considera-se que a garantia distribuída e pública, além de também ter a estrutura distribuída. Finalmente, o armazenamento de dados é realizado no próprio sistema, para cumprir o requisito de um órgão poder acessar documentos de outros. Vale ressaltar que diferentemente do sistema estoniano, o sistema proposto armazena apenas a autenticação do documento, mas não o seu conteúdo. A autenticação consiste no resultado de um algoritmo aplicado ao conteúdo do documento.

4 BLOCKCHAIN

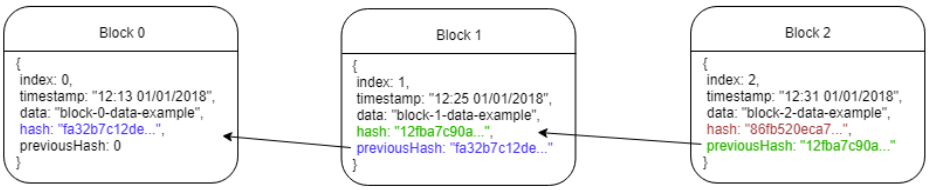
A estrutura de dados chamada de blockchain se assemelha a uma lista ligada. A estrutura, que tem os blocos como elementos atômicos, pode ser traduzida livremente como "cadeia de blocos". Estes têm estruturas bem definidas e invariavelmente possuem dados e metadados, entre os quais um *timestamp*, um código identificador característico do bloco e o identificador do bloco anterior. Este quesito constitui a semelhança com a lista ligada, pois um bloco referencia um outro para formar uma sequência. Porém, ao invés de um endereço de memória, a indicação se dá pelos códigos identificadores dos blocos em questão.

4.1 Imutabilidade de dados

A blockchain tem como base a teoria de criptografia, mais especificamente com a criação de *hash* e encriptação assimétrica. Uma função *hash* transforma um conjunto de dados de tamanho arbitrário para um tamanho fixo e é considerado suficientemente irreversível. Uma outra característica importante consolida-se na probabilidade ínfima de colisão de *hash*, isto é, o mesmo resultado ser obtido para conjunto de dados diferentes (SCHENEIER, 1996). Os códigos identificadores dos blocos são calculados por funções *hash*.

O *hash* característico do bloco é calculado a partir dos seus próprios dados, incluindo o *hash* do bloco anterior. Assim, a única maneira de criar um novo bloco é baseando-se no último da cadeia. Este fato cria a imutabilidade da estrutura de dados, visto que qualquer alteração nos dados de um bloco anterior causaria uma mudança no *hash* característico do mesmo e em todos os subsequentes.

Figura 6: Ilustração da estrutura blockchain



Fonte: Própria

4.2 Transparência e redundância

Uma rede de blockchain é constituída por diversos participantes, chamados de "nós", adotando uma mesma cadeia de blocos. Para a averiguação da autenticidade desta, necessariamente os nós precisam ter conhecimento de todos os blocos desde o primeiro, denominado "bloco gênesis", que não possui *hash* de um bloco anterior. Dessa maneira, a blockchain deve ser pública e transparente entre todos os nós participantes da rede. Não há outra maneira de processar a cadeia como um todo, sem a confiança em outra entidade, senão salvando os dados no próprio disco da máquina. Assim, há redundância de armazenamento de dados entre os nós participantes interessados em validar todo o histórico.

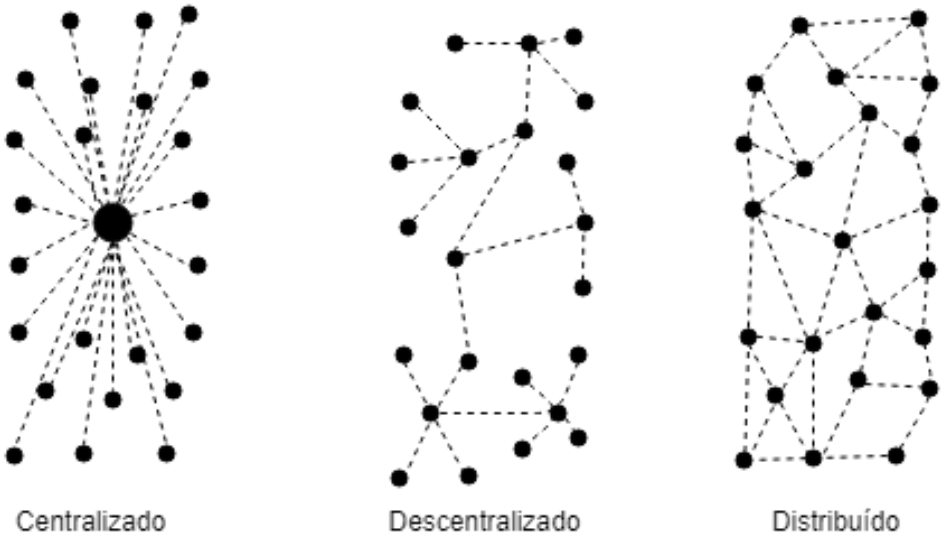
4.3 Controle de acesso

Além da inevitável transparência entre os nós, cada rede possui uma característica de controle de acesso dos participantes. Caso a rede blockchain tenha como função ser uma moeda de troca ou um banco de dados de comprovantes imutável, entende-se que é de benefício público a rede ser acessível a qualquer um que queira utilizar do recurso. Entretanto, se a aplicação for de armazenamento distribuído de dados sensíveis de uma empresa, faria mais sentido o acesso à rede ser controlado apenas aos *stakeholders* interessados. Dá-se o nome de redes de acesso controlado às redes privadas onde apenas os participantes aprovados podem interagir. Caso participantes possam entrar sem autorização, considera-se uma rede de acesso livre.

4.4 Centralização

No quesito de centralização de controle sobre uma rede qualquer, podem-se criar três categorias: centralizada, descentralizada e distribuída.

Figura 7: Ilustração da centralização



Fonte: Própria

A estrutura centralizada tem como maior exemplo as instituições financeiras tradicionais e são caracterizadas por um sistema que intermedeia todas as transações entre os usuários da rede. Neste caso, a adoção de uma blockchain como estrutura de dados não possui os benefícios atrelados ao efeito da distribuição, como a redundância e consenso. Como uma entidade central possui o poder sobre a rede, ela poderia alterar um dado passado e recalcular todos os *hashes* subsequentes como bem entendesse, tirando o sentido de adotar uma estrutura de dados como esta. O modelo descentralizado tem uma pequena quantidade de entidades como intermediadores das transações e pode ser considerado um meio termo entre a centralização e a distribuição total.

No outro extremo dos bancos tradicionais reside a maior quantidade de criptomoedas, no modelo distribuído. Nesta estrutura, nenhum nó possui poder de decisão intrínseco maior que os outros. A influência de cada nó sobre a rede depende da estrutura de consenso definida para a rede blockchain em questão.

4.5 Consenso

O consenso é constituído por um conjunto de regras e além de garantir a coesão dos dados, marginaliza qualquer intenção maliciosa. A regra mais básica do consenso pode ser considerada a necessidade de todos os novos blocos possuírem a estrutura de dados projetada. Isto significa que o novo bloco deve ter todos os atributos acordados e que sua referência ao *hash* do bloco anterior seja correta. Caso um nó afirme que o novo bloco possui um atributo diferente do esperado, a rede pode apenas ignorá-lo.

Como a estrutura da rede possui processamento descentralizado, existe a possibilidade de que haja divergências na criação de novos blocos. Caso dois nós incluam dados diferentes na criação de um novo bloco a ser alocado após o último, passam a existir duas cadeias válidas diferentes. Este problema, criado pela falta de uma entidade central, é resolvido a partir da adição de uma dificuldade de processamento de novos blocos ou de responsabilização consensual da entidade que deveria adicionar o bloco.

4.5.1 Proof of Work

A solução para as múltiplas cadeias chamada Proof of Work (PoW) tem como princípio a adição de uma tarefa computacional complexa na criação de novos blocos. O sucesso desta solução reside na facilidade de verificar que a complexa tarefa foi de fato realizada corretamente.

No caso do Bitcoin, a prova de processamento consiste na regra imposta de que o *hash* característico do bloco deve iniciar com um número determinado de caracteres zeros (NAKAMOTO, 2008). Esse objetivo é alcançado adicionando um número aleatório ao conjunto de dados que serão utilizados para o cálculo do *hash*. A quantidade requerida de zeros no início do *hash* aumenta exponencialmente a complexidade média de processamento e permite que o tempo entre a criação de blocos seja adaptado ao poder de processamento da rede. Este desafio dificulta qualquer alteração em blocos passados, já que seria necessário refazer toda prova de trabalho de todos os blocos subsequentes.

Caso haja diferentes cadeias válidas candidatas, o consenso consiste em adotar a com maior número de blocos. Como a cadeia mais longa representa o maior acúmulo de provas de trabalho, pode-se inferir que ela é adotada pela maioria do processamento da rede. Considerando que a maioria dos nós da rede são honestos, isto é, não tentam alterar maliciosamente alguma regra, conclui-se que a maior cadeia é a correta.

4.5.2 Proof of Authority

Outra solução de consenso para as *blockchains* é a Proof of Authority, ou Prova de Autoridade (PoA). Este método consiste em dar o poder de criação de blocos para entidades específicas da rede, de acordo com as suas reputações.

Diferente do modelo PoW, não é necessário que todos os validadores da rede despendam poder de processamento a cada bloco. Na rede do Bitcoin, que utiliza *Proof of Work*, o taxa de criação de *hashes* ultrapassa 3×10^{19} por segundo (Bitcoin.com, 2018). Considerando que cada bloco é gerado a cada 600 segundos, a quantidade de hashes calculados por bloco ultrapassa 1.8×10^{22}, com quase todos sendo inutilizados.

Na Prova de Autoridade, o validador escolhido para criar o bloco deve gerar apenas um *hash* e uma assinatura digital. A assinatura assegura que de fato o validador criou um bloco autêntico. Os outros validadores confirmam as informações do novo bloco e, se estiverem corretas, aceitam o bloco. Caso o novo bloco possua dados fraudulentos, o validador criador deixa de ser confiável, portanto seus futuros blocos não serão levados em consideração.

5 SISTEMA PROPOSTO

Rememorando o início do trabalho, o problema abordado consiste na ausência de autenticação de documentos entre diferentes sistemas de identificação. Os requisitos de sistema para a solução do problema foram definidos como:

- Documentos de identificação de diferentes emissores são armazenados no sistema;
- A autenticidade de cada documento é garantida pelo seu emissor;
- Qualquer sistema público ou privado pode consultar a autenticidade de um documento fornecido, independente do emissor do mesmo.

Após a revisão das práticas adotadas nos sistemas de identificação existentes, foi projetado um sistema de informação para atender a estes requisitos. Foram utilizadas metodologias de engenharia de software, como a linguagem UML (*Unified Modeling Language*) (ADDISON-WESLEY, 2005). O uso de uma linguagem de modelagem é especialmente relevante antes da implementação do sistema, pois facilita a compreensão e permite alterações estruturais com facilidade.

A especificação da UML contempla a criação de diversos diagramas, representando propriedades estruturais ou comportamentais do sistema. As definições estruturais têm como exemplo os diagramas de objetos, que definem estruturas de dados utilizados no sistema, bem como os diagramas de componentes, que descrevem a relação entre diferentes partes do sistema. Por outro lado, os diagramas comportamentais descrevem o funcionamento do sistema. Entre estes, foram utilizados os diagramas de casos de uso, para definir as funcionalidades do sistema, além de um diagrama de sequência, para estipular a execução da votação entre nós. Inicia-se o projeto do sistema pela definição dos atores:

5.1 Atores

O conjunto de atores do sistema de identificação pode ser sintetizado em três partes:

- Cidadão a ser identificado

  O cidadão é o indivíduo cuja identidade é salva no sistema de identificação e que utiliza os serviços do Provedor de Serviço.

- Provedor de Serviço

  O Provedor de Serviço pode ser caracterizado como entidade que deseja identificar corretamente o usuário para a prestação de um serviço específico. Dessa maneira, comunica-se com um Provedor de Identidade para a confirmação de autenticidade dos dados do usuário.

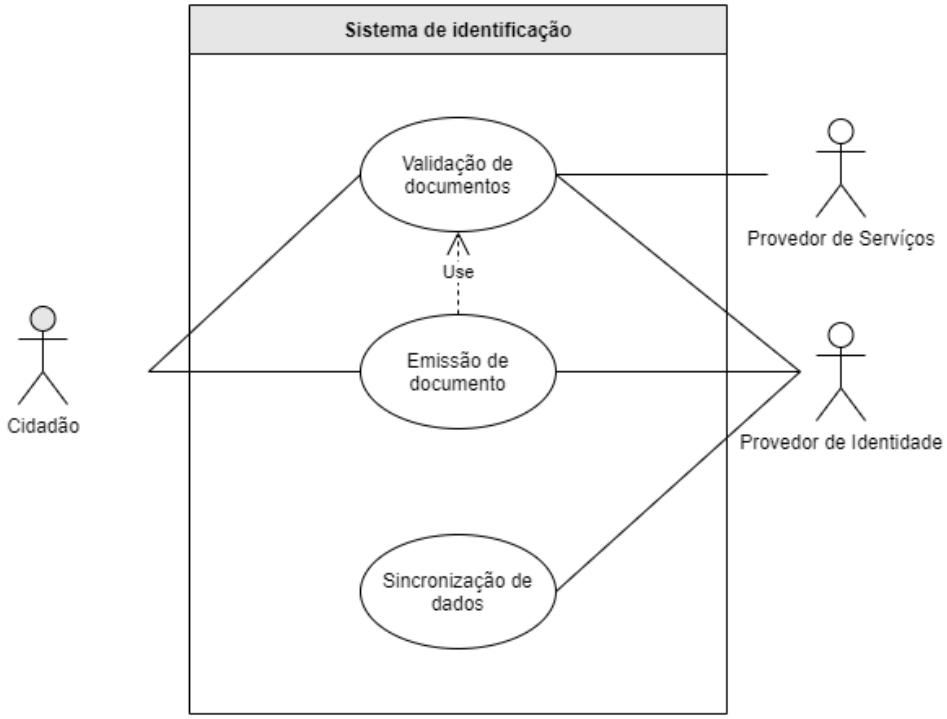
- Provedor de Identidade

  O Provedor de Identidade consiste na entidade que intermedeia todas as relações de criação e consulta de dados pessoais. No sistema proposto neste trabalho, define-se que este ator também fará o papel de autenticador dos dados.

5.2 Casos de uso

As funções essenciais do um sistema de identificação são sintetizadas nos seguintes casos de uso: emissão de documento, validação de documentos e sincronização de dados. Como o histórico de uma blockchain é imutável, não há edição ou exclusão de identidades. Em caso de correção, deve-se salvar o dado em um novo registro, mantendo o anterior no histórico.

Figura 8: Diagrama de casos de uso



Fonte: Própria

5.2.1 Emissão de documento

- Atores: cidadão, provedor de identidade
- Pré-condições: o provedor de identidade deve estar conectado à rede
- Pós-condições: o *hash* do documento do cidadão deve ser armazenado
- Fluxo principal

1. O cidadão requisita a emissão de algum documento, como RG ou passaporte, em uma instituição pública, representada pelo Provedor de Identidade. O cidadão deve fornecer dados pessoais para serem preenchidos no documento, como número do CPF ou RG.
2. O provedor de identidade autentica a validade dos dados informados no histórico local de blockchain
3. (a) Caso os dados sejam válidos, o provedor de identidade cria um novo bloco com o *hash* do novo documento e publica a atualização para os outros nós da rede. Após confirmação de todos os nós, armazena na blockchain do banco de dados local

(b) Caso haja algum dado inválido, o provedor de identidade rejeita a emissão do documento

5.2.2 Validação de documentos

- Atores: cidadão, provedor de serviço, provedor de identidade
- Pré-condições: o documento apresentado pelo cidadão ao provedor de serviço deve estar registrado no sistema
- Pós-condições: o provedor de serviço terá a confirmação de autenticidade do documento do cidadão
- Fluxo principal

  1. O cidadão reivindica um direito, apresentando documentos para o provedor de serviço
  2. O provedor de serviço envia os documentos a serem validados ao provedor de identidade
  3. O provedor de identidade gera o *hash* do documento e consulta no histórico da blockchain
  4. O provedor de identidade responde ao provedor de serviço se o documento está válido ou não

5.2.3 Sincronização de dados

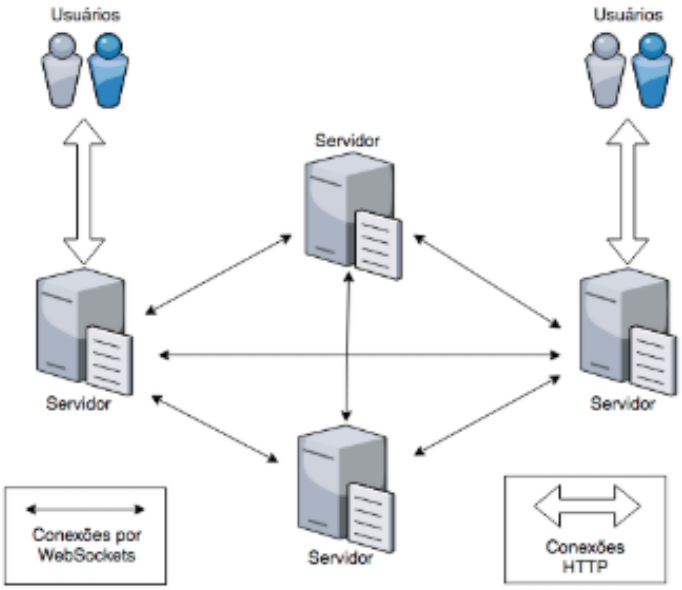
- Atores: provedores de identidade
- Pré-condições: os provedores de identidade devem estar conectados à rede
- Pós-condições: o PdI solicitante terá uma cópia do histórico de registros
- Fluxo principal

  1. O provedor de identidade requisita para outro PdI o histórico de blocos, desde um índice determinado
  2. O PdI requerido retorna o histórico de blocos desde o índice requisitado
  3. O PdI desatualizado recebe o histórico de blocos e verifica a autenticidade dos blocos recebidos. Em seguida, salva em seu histórico local.

5.3 Estrutura da rede

Cada nó da rede representa um Provedor de Identidade e será composto por um programa que se comunica com outros nós e atende requisições externas à rede. Deve ser utilizado um servidor HTTP que processa as requisições de emissões e consultas de documentos, feitas por cidadão ou Provedores de Identidade. Paralelamente, utiliza-se um servidor de WebSockets para a comunicação em tempo real entre os nós da rede.

Figura 9: Ilustração da arquitetura da rede de servidores



Fonte: Própria

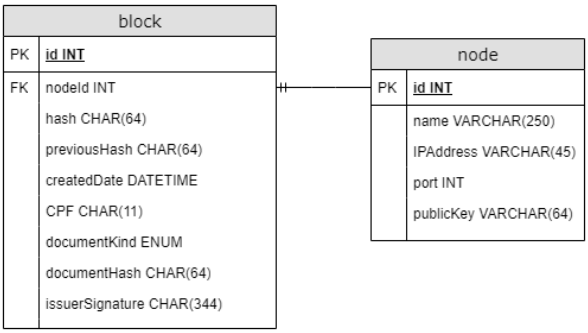
5.4 Estrutura de dados

O banco de dados relacional tem como função salvar tanto os dados referentes aos documentos quanto aos Provedores de Identidade da rede blockchain. Para tal, a modelagem foi feita em duas tabelas diferentes:

Tabela *block*: implementação da sequência de blocos da blockchain. Cada bloco contém informações relativas a um único documento de um cidadão. A propriedade de distinção entre cidadãos é o CPF.

Tabela *node*: lista de todos os nós participantes da rede, com seus respectivos nomes, endereços IP e chave pública para confirmação de autenticidade.

Figura 10: Modelagem do banco de dados



Fonte: Própria

Os valores permitidos na coluna *documentKind* da tabela *block*, são definidos na tabela a seguir:

Tabela 4: Tipos de documentos no sistema

Descrição	Valor da coluna documentKind
Número do RG para cada estado, com sufixo do código do UF	RG_[UF]_NUMBER
Número da CNH	CNH_NUMBER
Número do Passaporte	PASSPORT_NUMBER

5.5 Consenso

O consenso da rede projetada se baseia no conceito de *Proof of Authority*, ou Prova de Autoridade. Para viabilizar este modelo, dois conceitos são essenciais: a garantia da autenticidade e a ordem de inserção dos blocos.

5.5.1 Criação do bloco

Cada Provedor de Identidade terá uma chave privada e uma chave pública, geradas no padrão PKCS #1 (MORIARTY et al., 2016). As chaves públicas de todos nós são disponibilizadas para todos os PdIs, a fim de validar a autenticidade das assinaturas dos blocos que receberem. Cada nó da rede deve manter a sua chave privada como variável de ambiente e não transmiti-la em nenhuma situação.

Para calcular o *hash* do bloco, os nós devem formatar as informações a serem inseridas

com a função JSON.stringify e aplicar o algoritmo SHA256. Em seguida, o emissor assina o bloco com a sua chave privada, utilizando o paradigma *RSA hash-and-sign*, que permite a assinatura de *strings* com tamanhos arbitrários (KATZAND; LINDELL, 2007). Dessa maneira, é impossível alterar alguma informação do bloco sem alterar o *hash* e assinatura do mesmo. Vale notar também que o *hash* também é invalidado caso seja utilizada uma chave privada incorreta.

Os dados do *payload* e seus formatos são definidos no JSON a seguir:

```
{
    id: number,
    previousHash: string,
    createdDate: string,
    CPF: string,
    documentKind: string,
    documentHash: string
}
```

O código a seguir demonstra um exemplo desta geração, utilizando JavaScript e a biblioteca node-forge:

```
const forge = require("node-forge");
const rsa = forge.pki.rsa;

const newBlockPayload = {
  id: 1234,
  previousHash: "5fd924625f6ab16a19cc9807c7c506ae1813490e4ba675f843d5a10e0baacdb8",
  createdDate: "2021-01-01T12:34:56",
  CPF: "31415926590",
  documentKind: "PASSPORT_NUMBER",
  documentHash: "c5f55c58ce7d951b77810a2a2dd709484d07f1977e4e14033a72c1a7740168c8"
}

// ------------------------------------------------------------------------------
// [PdI emissor/receptores] Criacao de hash do bloco
const stringifiedPayload = JSON.stringify(newBlockPayload);
const md = forge.md.sha256.create();
md.update(stringifiedPayload, "utf-8");
const newBlockHash = md.digest();

console.log(newBlockHash.toHex())
// Resultado: bd16bc83b198cb3e0f35111cab1d05cd04a1ea619c6e0b3117b9337f7ba29ace


// ------------------------------------------------------------------------------
// [PdI emissor] Criacao da assinatura bloco pelo PdI emissor a partir dos dados
const { privateKey, publicKey } = rsa.generateKeyPair({ bits: 2048 });

const newBlockSignature = privateKey.sign(md);
console.log(forge.util.encode64(newBlockSignature))
// Resultado: RFmKBXZ+wfySsmxlHGrK7ehw+Up9gav1c2B96AEkTA8XNWjHyuvliS63qjAw/5yNfqU+
    jCQqoDarVmIUICM1Zauwastsd7mUtOQyiwnDLgphKazqQRRhvCX1/X9qPjMYmP4FBFnIDHWDS/
    rKIFEI6FMPouDy+PH5diArwE6OVDqpofc4CHrkgwLG6x1zQl9YB5BVA/
    RxwLnswZPovlXAYNOw0G6uwXf5IQkbxGa/3rD8wP8BFsukqVrEIJPrtW/7uMZFku+
    FHWNWAx8aYImphRYXmEf0/cBF+vMiaU0wKK5F7jNt//fV4AzgRqKhXKl14Dn/o82BcPtP4LNzwzrWnQ==


// ------------------------------------------------------------------------------
// [PdIs receptores] Verificacao de autenticidade da assinatura
const verified = publicKey.verify(newBlockHash.bytes(), newBlockSignature);
console.log(verified)
// Resultado: true
```

Os nós que receberem os dados do bloco novo usam o mesmo algoritmo SHA256 para calcular o *hash* do *payload*. Em seguida, utilizam a chave pública do PdI emissor para verificar se foi o mesmo que criou o bloco de fato.

5.5.2 Transmissão do bloco

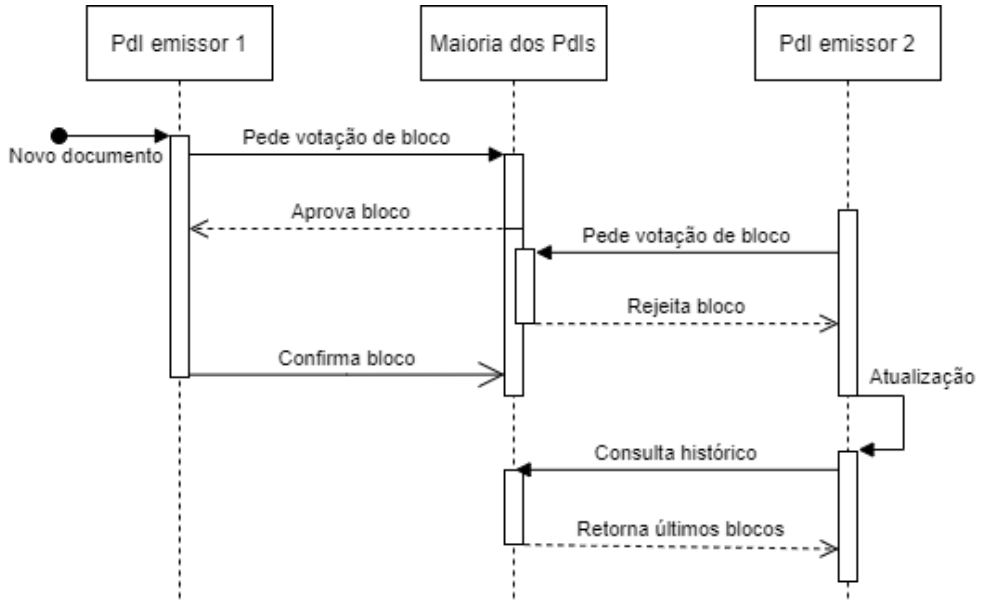
Por haver sincronização de dados entre os participantes da rede, é necessário haver um acordo entre eles na criação simultânea de blocos. Caso contrário, a ordenação da

corrente de blocos seria diferente em cada um, invalidando o cálculo correto dos *hashes*. Além disso, não há hierarquia entre os participantes, de modo que é necessária uma organização temporal na criação do bloco.

A seguir é explica-se o fluxo de criação dos blocos e sua transmissão na rede:

1. Provedor de Identidade emissor gera o bloco com o *hash* e assinatura e envia um pedido de inserção de bloco para todos os nós da rede
2. PdIs consultados verificam se está de acordo com ordem e assinatura. Criam um bloco **provisório** nos seus bancos de dados locais e respondem para o emissor que aprovam o bloco
3. A partir do momento que o emissor envia o pedido, aguarda até que a maioria dos nós respondam ou que transcorram 1000ms
   (a) Se a maioria dos blocos online aprovar dentro do tempo limite, o emissor envia uma nova mensagem para os nós consolidarem o bloco
   (b) Se o bloco não for aprovado ou os nós não obtiverem a confirmação de consolidação dentro de 1000ms, o bloco é desconsiderado. Neste caso, o emissor deve realizar uma atualização de dados para corrigir o seu histórico.

Figura 11: Diagrama de sequência do consenso



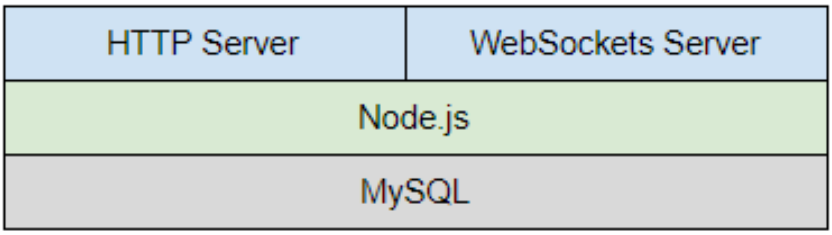
Fonte: Própria

6 DESENVOLVIMENTO DE PROTÓTIPO

O desenvolvimento do protótipo visou provar o conceito de servidores diferentes serem capazes de compartilhar uma mesma base de dados. Para isso, criou-se o servidor com as funções básicas do sistema de identificação e um *website* para a sua interface.

O servidor foi desenvolvido utilizando o Node.js, que suporta dezenas de milhares de conexões simultâneas (CHHETRI, 2016). A tecnologia utiliza o interpretador V8 JavaScript Engine, criada pela Google e utilizada no Google Chrome (Node.js Foundation, 2018). Para o armazenamento de longo prazo, foi utilizado o banco de dados relacional MySQL.

Figura 12: Conjunto de tecnologias do servidor (*tech stack*)



Fonte: Própria

Foi desenvolvido o *software* do servidor com os serviços tanto externos quanto internos à rede de servidores. Para a comunicação intra-rede, foi criado em cada nó um servidor de *WebSockets*. Para a comunicação extra-rede, foram criados *webservices* HTTP para emissão e consulta de documentos.

6.1 Serviços HTTP

Os serviços HTTP fazem a interface entre os dados da blockchain e o Provedor de Serviço ou Identidade. Foram desenvolvidas duas requisições para a prova de conceito, seguindo o padrão REST (FIELDING, 2000):

Adição de documentos

Envia requisição a um nó da rede para salvar um hash da identidade.

POST /document

Exemplo de corpo de requisição:

```
{
    CPF: "31415926590",
    kind: "RG_SP",
    content: "106245193"
}
```

Exemplo de resposta com status 200:

```
{
    "document": {
        "CPF": "31415926590",
        "kind": "RG_SP",
        "content": "106245193",
        "hash": "8c56e821c21923d5d95d39b9bbc0b1c4cfee68f8cefdc314e656b22d05a62687"
    },
    "id": 2,
    "previousHash": "539f335f4d27740ffa31951ccdcb300eac0f192f61d6a8ad917b49f654b04629",
    "createdDate": "2021-10-29T01:29:00.000Z",
    "hash": "7c1bbcfbc16696a899351b597a4dd7a7bbecff01aaf72a2d5e00926903b1abee",
    "issuerSignature": "YdpbaFwQ4nh+3
        HgzzOIBrwWVWDu1jPXfYvDEvvybZ4ZjUhHHyJAk6D4xJW6xhq1MbDTmUkXDwEKKXxatiBSwsbNYA3
    YAEGw9hBuNQTZBe+o+ho06jLwCs+C8QI8hIVso1ghqONUuNZZErgKOj7c9q1yr5EXGZDHzCyobxKNKBas+
        UsGBZCWOKwzaGxkhyQ8NXqzomg7WP81qeqDH5MHByE9Izlr2Fdvo7pauQTkS+YN60Rk0utdoI6Xx+
        PMf8Q+i4cmIoG6wNQgYvfCuA3ojpm+2mh43nJsEHM+P/y6+wLu+5+MIidxavB5RnjOBG0Ot+
        RtlvMJEoVvGF6j/yKaP3A==",
    "node": {
        "id": 1
    }
}
```

Exemplo de resposta com status 504:

```
Bloco nao foi salvo na rede
```

Exemplo de resposta com status 409:

```
Documento ja cadastrado
```

Consulta de validade documentos

GET /document

Envia requisição a um nó da rede para verificar se o conjunto de documentos são válidos.

Exemplo de corpo de requisição (parâmetros da URL):

```
    CPF: "31415926590"
    kind: "RG_SP"
    content: "106245193"
```

Exemplo de resposta com status 200:

```
{
    "createdDate": "2021-11-29T01:29:00.000Z",
    "node": {
        "name": "Primeiro no"
    }
}
```

Exemplo de resposta com status 404:

```
Documento nao encontrado
```

6.2 Comunicação por *WebSockets*

Neste protótipo, cada nó se conecta com todos os outros da rede. Como a tabela *node* do banco de dados armazena o endereço IP e porta de cada nó, o servidor pode tentar se conectar com os outros assim que foi inicializado.

Uma vez estabelecida a conexão entre os nós por *WebSockets*, a comunicação se dá por troca de mensagens em formato JSON. O protocolo criado define as mensagens com a seguinte estrutura:

```
{
    event: string,
    data: any
}
```

A propriedade *event* do JSON tem a possibilidade de ter valores diferentes:

LOCK_BLOCK

Envio de um novo bloco provisório a ser validado pelos outros nós da rede. Neste caso, o objeto em *data* consiste no novo bloco a ser avaliado e adicionado à blockchain local.

Exemplo de mensagem:

```
{
    event: "lockBlock",
    data: {
        id: 1234,
        hash: "bd16bc83b198cb3e0f35111cab1d05cd04a1ea619c6e0b3117b9337f7ba29ace",
        previousHash: "5fd924625f6ab16a19cc9807c7c506ae1813490e4ba675f843d5a10e0baacdb8",
        createdDate: "2021-01-01T12:34:56",
        CPF: "31415926590",
        documentKind: "PASSPORT_NUMBER",
        documentHash: "c5f55c58ce7d951b77810a2a2dd709484d07f1977e4e14033a72c1a7740168c8",
        issuerSignature: "RFmKBXZ+wfySsmxlHGrK7ehw+Up9gav1c2B96AEkTA8XNWjHyuvliS63qjAw/5
            yNfqU+jCQqoDarVmIUICM1Zauwastsd7mUtOQyiwnDLgphKazqQRRhvCX1/
            X9qPjMYmP4FBFnIDHWDS/rKIFEI6FMPouDy+PH5diArwE6OVDqpofc4CHrkgwLG6x1zQl9YB5BVA/
            RxwLnswZPovlXAYNOw0G6uwXf5IQkbxGa/3rD8wP8BFsukqVrEIJPrtW/7uMZFku+
            FHWNWAx8aYImphRYXmEf0/cBF+vMiaU0wKK5F7jNt// fV4AzgRqKhXKl14Dn/
            o82BcPtP4LNzwzrWnQ=="
    }
}
```

BLOCK_LOCKED

Resposta à mensagem LOCK_BLOCK em caso de aprovação das informações do bloco e da possibilidade de inserção na blockchain.

Exemplo de mensagem:

```
{
    event: "blockLocked",
    data: {
        id: 1234,
        hash: "bd16bc83b198cb3e0f35111cab1d05cd04a1ea619c6e0b3117b9337f7ba29ace"
    }
}
```

CONSOLIDADE_BLOCK

Mensagem enviada no caso de o criador do bloco receber a confirmação de criação do bloco da maioria dos nós.

Exemplo de mensagem:

```
{
    event: CONSOLIDADE_BLOCK,
    data: {
        id: 1234,
        hash: "bd16bc83b198cb3e0f35111cab1d05cd04a1ea619c6e0b3117b9337f7ba29ace"
    }
}
```

GET_BLOCKS_SINCE_ID

Esta mensagem constitui a requisição de todos os blocos a partir de um índice espe-

cificado na propriedade *data*.

Exemplo de mensagem:

```
{
    event: GET_BLOCKS_SINCE_ID,
    data: {
        id: 1234
    }
}
```

BLOCKS_SINCE_ID

Resposta à mensagem GET_BLOCKS_SINCE_ID, retornando a listagem de blocos da *blockhain*.

Exemplo de mensagem:

```
{
    event: VALIDATE_BLOCK,
    data: [{
        id: 1234,
        hash: "bd16bc83b198cb3e0f35111cab1d05cd04a1ea619c6e0b3117b9337f7ba29ace",
        previousHash: "5fd924625f6ab16a19cc9807c7c506ae1813490e4ba675f843d5a10e0baacdb8",
        createdDate: "2021-01-01T12:34:56",
        CPF: "31415926590",
        documentKind: "PASSPORT_NUMBER",
        documentHash: "c5f55c58ce7d951b77810a2a2dd709484d07f1977e4e14033a72c1a7740168c8",
        issuerSignature: "RFmKBXZ+wfySsmxlHGrK7ehw+Up9gav1c2B96AEkTA8XNWjHyuvliS63qjAw/5
            yNfqU+jCQqoDarVmIUICM1Zauwastsd7mUtOQyiwnDLgphKazqQRRhvCX1/
            X9qPjMYmP4FBFnIDHWDS/rKIFEI6FMPouDy+PH5diArwE6OVDqpofc4CHrkgwLG6x1zQl9YB5BVA/
            RxwLnswZPovlXAYNOw0G6uwXf5IQkbxGa/3rD8wP8BFsukqVrEIJPrtW/7uMZFku+
            FHWNWAx8aYImphRYXmEf0/cBF+vMiaU0wKK5F7jNt// fV4AzgRqKhXKl14Dn/
            o82BcPtP4LNzwzrWnQ=="
    },{
        id: 1235,
        hash: "7301da44a9cac069bbfcacf54f6215893e1272abc266f777cbc589df391f58fe",
        previousHash: "bd16bc83b198cb3e0f35111cab1d05cd04a1ea619c6e0b3117b9337f7ba29ace",
        createdDate: "2021-01-01T12:34:56",
        CPF: "31415926590",
        documentKind: "RG_SP",
        documentHash: "c5f55c58ce7d951b77810a2a2dd709484d07f1977e4e14033a72c1a7740168c8",
        issuerSignature: "vVhUYYgQDWPESsznprzCua9W0dIKU4c9VNDgIhAzaML+/mCxsCfhKo6R/
            mBx8IqYcWjzeXojVO3gVBxU6fWkJ9UyFcNhn5vMIo5prYpPZlCI4oqgk9z7gO1TKvKkw/
            tcnATImUA4GEN3HhdtAn1g2ALPCcZiSj1bC6CHuz6/
            ZZqXpUeh6MV8qALiJ5yhLOVZeoengToTkROinEdG55fS68QHBG7yWljyNFGxHyKcI+7
            j6rxOwtFwgs0glgFzoghP38RBCWm701f9NCr6tt9ejBf+Xbk/F8ty30KMWEBoWb+
            pcQTrRQ1aoFNCauhCvoSyJ3ugYa6zVuKTVqhiefMj9A=="
    }]
}
```

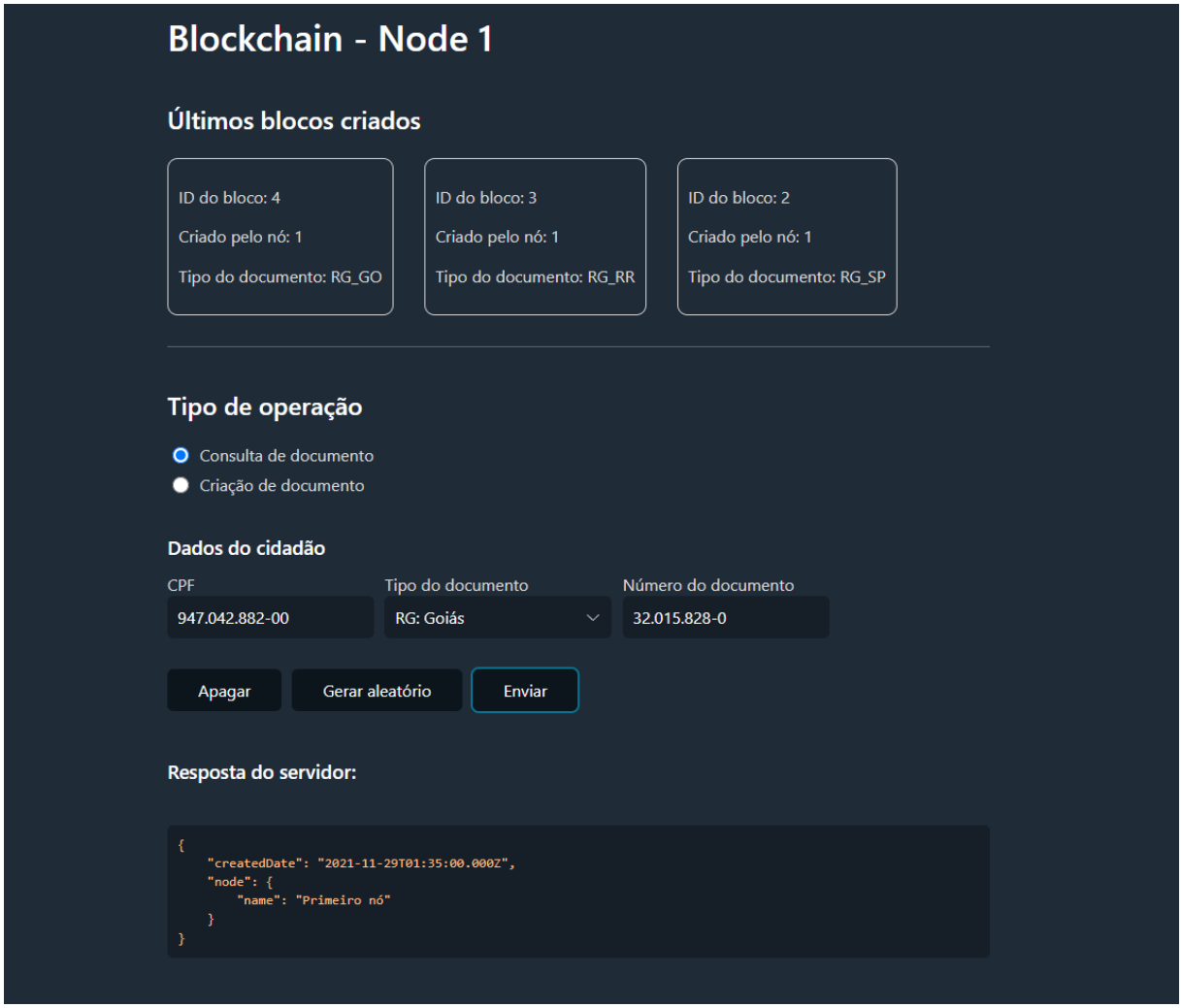
6.3 *Website*

O *website* foi criado com o intuito de testar os serviços HTTP do servidor. Nele é possível utilizar o sistema atuando como um Provedor de Identidade ou como um Provedor de Serviço.

Para facilitar os testes, tanto a criação quanto a consulta de documentos estão livres. Há seletores de tipo de documento a serem validados, bem como a caixa de texto para escrever o seu conteúdo.

Para facilitar o desenvolvimento, utilizou-se o *framework* Vue.js.

Figura 13: Exemplo da página web desenvolvida



Fonte: Própria

7 RESULTADOS E ANÁLISE

Para esta prova de conceito, os testes foram realizados com quatro nós da rede sendo executados no mesmo computador. O mesmo código foi utilizado entre eles, com a diferenciação de uma variável de ambiente, para identificar o número de cada um. Os processos executaram de forma independente entre eles e a cada um foi atribuído um conjunto de portas de rede diferentes. A conexão entre processos foi realizada por WebSockets, utilizando as portas de rede assinaladas para o protocolo de comunicação específico. Além disso, cada subsistema serviu a página web e as suas requisições HTTP em outras portas de rede.

Foram criados também bancos de dados isolados entre si para o armazenamento de cada servidor. Os bancos também executaram no mesmo computador. Baseado na variável de ambiente de inicialização do servidor, cada processo conectou-se ao banco de dados correto, além de carregar o arquivo de chaves públicas e privadas utilizadas nas funções criptográficas.

Utilizaram-se quatro servidores na rede blockchain, visto que é o número mínimo para o teste de consenso. Durante a criação de um bloco, o nó emissor envia uma mensagem de votação para todos os outros servidores. Caso houvesse apenas outros dois participantes da rede, a maioria necessária para aprovação do bloco seria de dois, sendo equivalente a todos os participantes. O cenário não contemplaria o teste de vitória da maioria com rejeição de um dos participantes. A rejeição pode ocorrer pela ausência de dados atualizados ou durante a criação simultânea de blocos. O nó que rejeitou o bloco ainda deve salvá-lo, caso o consenso aprove a sua criação.

Com o sistema em funcionamento, foram executados cenários semelhantes aos reais para teste dos casos de uso. Como estes foram criados com base nos requisitos de projeto, a validação do funcionamento dos mesmos confirma o cumprimento dos requisitos do sistema.

7.1 Registro de um documento válido

- Ator simulado: funcionário da Secretaria de Segurança Pública de São Paulo atuando como um Provedor de Identidade
- Caso de uso: Emissão de documento
- Metodologia: O teste consistiu no registro de uma carteira de identidade (RG) de um indivíduo. A inserção foi feita pelo website, utilizando a funcionalidade de criação de documento. Colocou-se o número de CPF e o número do RG nos campos de texto, além da seleção do tipo de documento como RG de São Paulo.
- Resultados: O resultado obtido foi o esperado: o nó que recebeu a requisição verificou a inexistência do conjunto de documentos no banco de dados, criou o bloco e enviou a mensagem para os nós conectados. Estes receberam a mensagem, verificaram a validade do bloco e adicionaram à sua blockchain local. Com a confirmação dos outros blocos, o nó emissor também armazenou o novo bloco ao seu banco de dados.

7.2 Validação de documento emitido por outro nó

- Ator simulado: funcionário do DETRAN atuando como um Provedor de Serviço
- Caso de uso: Validação de documento
- Metodologia: O teste representa o cenário da verificação de validade dos documentos fornecidos antes da emissão de uma Carteira Nacional de Habilitação pelo DETRAN. O cidadão apresentou o documento de RG constando o número de CPF, conforme procedimento da criação da CNH. Antes de iniciar o processo de criação da CNH, o funcionário deve averiguar a autenticidade dos dados fornecidos. Assim, entrou no website, escolheu a funcionalidade de consulta de documentos e preencheu o formulário com as informações pessoais do cidadão. O documento de identidade foi emitido por outro nó, de modo que o teste consistiu na verificação da existência do mesmo no histórico local.
- Resultados: Como o histórico de blocos é replicado entre todos os nós da rede, verificou-se a existência do documento no banco de dados. A presença do documento validou não apenas a inserção prévia do documento, mas também o seu vínculo com o CPF e o estado de origem. É possível, por exemplo, que haja um mesmo número

de RG vinculado a outro CPF, desde que seja emitido em outro estado, isto é, definido com um diferente tipo de documento.

7.3 Registro de um documento duplicado

- Ator simulado: funcionário da Secretaria de Segurança Pública de São Paulo atuando como um Provedor de Identidade
- Caso de uso: Emissão de documento
- Metodologia: O teste consistiu na tentativa de registro de um número de identidade (RG) já existente no sistema, mas vinculado a outro CPF. O cenário simula a tentativa de fraude por parte do cidadão que requereu a identidade, considerando que forneceu documentos com informações adulteradas. A inserção foi feita pelo website, utilizando a funcionalidade de criação de documento. Colocou-se o número de CPF e o número do RG nos campos de texto, além da seleção do tipo de documento como RG de São Paulo.
- Resultados: O nó que recebeu a requisição constatou a existência prévia do documento no histórico de blockchain. Como não pode haver um mesmo número de documento para o mesmo tipo, a verificação foi realizada antes da propagação da mensagem para os outros nós da rede. Dessa maneira, a emissão do novo documento foi recusada e as informações fornecidas pelo cidadão podem ser investigadas.

7.4 Conexão de um nó desatualizado à rede

- Ator simulado: Provedor de Identidade
- Caso de uso: Sincronização de dados
- Metodologia: Com objetivo de avaliar a robustez do sistema, foi mantido um Provedor de Identidade sem conexão à rede blockchain. Enquanto isso, foram inseridos diversos documentos nos outros nós, gerando uma defasagem de dados entre eles. Foi então conectado o Provedor de Identidade à rede, para testar a atualização de dados.
- Resultados: Ao inicializar o servidor, o Provedor de Identidade solicitou o histórico de blockchain dos outros nós desde o seu último registro. Ao receber os dados,

verificou a autenticidade de cada um dos blocos recebidos e salvou-os no seu banco de dados, tornando-o atualizado.

A possibilidade de sincronização dos dados assegura a preservação do histórico do sistema em diversas eventualidades. É possível, por exemplo, se recuperar da situação em que a conexão foi perdida em um dos nós da rede, gerando a defasagem de dados. Além disso, garante que novos nós possam ser adicionados à rede, dado que atualizam seu histórico antes de atuar como um criador de documentos.

A verificação de autenticidade dos blocos recebidos na atualização é importante para evitar vulnerabilidades no sistema. Caso não houvesse a validação da assinatura digital de cada bloco recebido, o sistema ficaria suscetível a receber informações incorretas na inicialização. Agentes maliciosos poderiam se aproveitar da vulnerabilidade, de alguma maneira interrompendo as conexões de um dos nós e enviando blocos fraudulentos na sua atualização de dados.

8 CONCLUSÃO

No início do trabalho foi identificado que alguns tipos de crimes são facilitados por falhas em sistemas de identificação. Verificou-se que esses crimes possuem grande relevância, pois causam prejuízos financeiros globalmente e podem estar relacionados com tráfico, homicídios e imigração ilegal. Supôs-se que estes crimes estudados teriam sido dificultados pela comunicação entre diferentes sistemas de identificação para autenticar os documentos utilizados pelos criminosos. Com base nesta hipótese, foram definidos requisitos de projeto para a solução do problema apresentado.

Foram estudados e analisados diferentes sistemas de identificação. Estes possuíam diferentes países de origem, bem como padrões adotados e tecnologias utilizadas. Foi pesquisada também a progressão dos sistemas de identificação brasileiros que visavam a centralização de dados, iniciada em 1997. Entre as tecnologias e metodologias utilizadas nos sistemas, destacou-se o uso de blockchain, pela possibilidade de confiança distribuída entre participantes do sistema. O trabalho examinou a origem, propriedades e aplicações de blockchain. Entre as possibilidades de configuração da rede, foram escolhidos os atributos que mais se adequaram ao problema.

Com base nos requisitos de projeto definidos e na análise de outros sistemas de identificação, foi proposto um sistema. O projeto utilizou metodologias de engenharia de software, como a definição de casos de uso, atores, arquitetura do sistema e testes. Os casos de uso foram definidos como a criação de documento, validação de documento e a sincronização de dados. Com as três funcionalidades, o sistema cumpre os requisitos do projeto para a resolução do problema estudado.

Após projeto do sistema, foi desenvolvido o protótipo que implementa a arquitetura e especificações estabelecidas. O protótipo foi composto de três partes, sendo elas a página web, o servidor e o banco de dados. O último foi utilizado para armazenamento de dados, controlado pela lógica do servidor. A página web foi utilizada para a interação do usuário final com o sistema.

O desenvolvimento do protótipo permitiu a realização de testes para confirmação do funcionamento dos casos de uso. Utilizou-se a página web para simular a interação de um provedor de serviço ou de identidade com o sistema. Além disso, foi testada a sincronização de dados ao conectar um novo nó, com dados defasados. Os testes apresentaram sucesso no cumprimento dos casos de uso e, por consequência, dos requisitos de sistema.

Salienta-se que os testes foram executados no computador do autor do trabalho, isto é, em um ambiente controlado. Para testes de desempenho mais aprofundados, seria necessário adicionar latência na comunicação entre os participantes da rede, a fim de simular o atraso da comunicação causada pela distância física entre os servidores. Além disso, a comunicação dos componentes do sistema, isto é, entre servidores e entre *website* e servidor, não utilizou encriptação no protótipo. Para aplicações reais, sugere-se a utilização de protocolos seguros de comunicação, com o intuito de evitar vulnerabilidades na transmissão de mensagens. Finalmente, a geração e distribuição do par de chaves criptográficas também exige diligência, dado que a verificação de autenticidade dos documentos se baseia na posse da chave privada restrita ao seu legítimo controlador.

Para a aplicação real do sistema, seria necessária a inclusão de algumas funcionalidades secundárias. Pela ausência de controle de acesso, qualquer indivíduo é capaz de utilizar o sistema projetado. Seria relevante a criação de acessos pessoais e intransferíveis, vinculados às ações permitidas no sistema, seja consulta, criação de documentos ou ambos. Este controle poderia também segmentar a permissão de criação por tipo de documento, a fim de manter a responsabilidade de cada tipo restrita a cada órgão público. Ademais, o sistema considera a impossibilidade de erros de inserção de documentos. Sendo o histórico da blockchain imutável, o caso extremo de cancelamento ou substituição de um documento registrado não foi levado em consideração.

Em suma, este trabalho consistiu no estudo de um grave problema de identificação civil e na proposta de sua solução utilizando a tecnologia de blockchain. A vulnerabilidade estudada se manifesta na falha de autenticação de documentos emitidos por diferentes entidades e o sistema proposto cumpriu os requisitos para solucionar o problema.

REFERÊNCIAS

Universidade de Brasília. *RT Custos Econômicos e Sociais das Falhas*. [S.l.], 2014. Disponível em: <http://justica.gov.br/Acesso/governanca/pdfs/projeto-gestao-integrada>.

United Nations Office on Drugs and Crime. *World drug report*. [s.n.], 2011. v. 3. ISSN 1084-4791. ISBN 9789211482621. Disponível em: <https://www.unodc.org/documents/data-and-analysis/WDR2011/World/Drug/Report/2011/ebook.pdf>.

Presidência da República. *Lei Nº 9.454*. 1997. Disponível em: <http://planalto.gov.br/ccivil/03/leis/l9454.htm>.

CONGRESSO NACIONAL. *PL Nº 9.929*. 2015. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0bokwpkiy6rs6odoxyq43nzrk7676902.node0?codteor=1342951&filename=Tramitacao-PL+1775/2015>.

Presidência da República. *Lei Nº 13.444*. 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm>.

MARTINS, C. *Delegacia do PR investiga como Cupertino tirou RG com dados falsos*. 2014. Disponível em: <https://noticias.r7.com/brasil/pizzolato-emitiu-passaporte-falso-quatro-anos-antes-do-julgamento-do-mensalao-05022014>.

R7. *Delegacia do PR investiga como Cupertino tirou RG com dados falsos*. 2020. Disponível em: <https://noticias.r7.com/sao-paulo/delegacia-do-pr-investiga-como-cupertino-tirou-rg-com-dados-falsos-28102020>.

TEIXEIRA, L. B. *Fraudadores do INSS ganham aposentadoria com RG e certidão falsos*. 2019. Disponível em: <https://economia.uol.com.br/noticias/redacao/2019/01/24/principais-fraudes-contra-previdencia-falsificacao-documentos.htm>.

MAZZINI, L. *Força-Tarefa Previdenciária evita prejuízo de R$ 1,3 bi*. 2019. Disponível em: <https://jornaldebrasilia.com.br/blogs-e-colunas/coluna-esplanada/forca-tarefa-previdenciaria-evita-prejuizo-de-r-13-bi/>.

MAYNARD, N.; MORROW, S. *ONLINE PAYMENT FRAUD Reprint for Experian Report Author*. 2021. Disponível em: <https://www.experian.com/blogs/global-insights/wp-content/uploads/2021/07/Online-Payment-Fraud-2021-Experian.pdf>.

EXPERIAN, S. *Pesquisa Global de Identidade e Fraude 2021 Proteger e promover o engajamento dos clientes na nova era digital*. 2021. Disponível em: <https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2021/06/Pesquisa-Global-de-Identidade-e-Fraude-2021.pdf>.

ETHNEWS. *Brazil's Ministry Of Planning Reveals Ethereum-Based Proof Of Concept For Verifying Identity*. 2017. Disponível em: <https://www.ethnews.com/brazils-ministry-of-planning-reveals-ethereum-based-proof-of-concept-for-verifying-identity>.

International Business Times. *Ethereum identity system uPort working with Brazil's Ministry of Planning*. 2017. Disponível em: <https://www.ibtimes.co.uk/ethereum-identity-system-uport-working-brazils-ministry-planning-1636253>.

Federal Office for Information Security of Germany. *BSI - The electronic ID card*. 2010. Disponível em: <https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/eIDcard/eIDcard/node.html>.

HUGHES, J. et al. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. 2005. Disponível em: <http://docs.oasis-open.org/security/saml/v2.0/>.

Universidade de Brasília. *RT Estratégias Nacionais de Gestão de Identidade na Europa*. [S.l.], 2015. Disponível em: <http://justica.gov.br/Acesso/governanca/pdfs/estrutura-documental>.

DELL'INTERNO, M. *Carta di Identità Elettronica*. 2001. Disponível em: <http://www.cartaidentita.interno.gov.it/caratteristiche-del-documento/>.

European Comission. eGovernment in Italy. 2016. Disponível em: <https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernmentinItaly-February2016-18/00-v1/00.pdf>.

Agenzia per l'Italia Digitale. SPID REGOLE TECNICHE. 2014. Disponível em: <https://www.agid.gov.it/sites/default/files/repository/files/regole/tecniche/spid/regole/tecniche/v0/1.pdf>.

Italian Digital Transform Team. *Public Digital Identity System (SPID)*. 2018. Disponível em: <https://teamdigitale.governo.it/en/projects/digital-identity.htm>.

ESTONIA. *e-Identity | e-Estonia*. 2018. Disponível em: <https://e-estonia.com/solutions/e-identity/>.

Civic Technologies. *Civic White Paper*. 2017. 1–18 p. Disponível em: <https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf>.

UPORT. *uPort Specs*. 2018. Disponível em: <https://developer.uport.me/readme>.

BRAENDGAARD, P.; UPORT. *Different Approaches to Ethereum Identity Standards*. 2018. Disponível em: <https://medium.com/uport/different-approaches-to-ethereum-identity-standards-a09488347c87>.

JONES, M. et al. RFC 7519 - JSON Web Token - JWT. 2015. Disponível em: <https://tools.ietf.org/pdf/rfc7519.pdf>.

BENET, J. IPFS - Content Addressed, Versioned, P2P File System. 2017. Disponível em: <https://ipfs.io/>.

UPORT. 2021. Disponível em: <https://serto.medium.com/uport-is-now-serto-df9c73d545e6>.

SCHENEIER, B. *Appled Criptography: Protocols, Algorithms, and Source Code in C*. [S.l.: s.n.], 1996. 675 p.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. p. 1–9, 2008. Disponível em: <www.bitcoin.org>.

ADDISON-WESLEY. *Unified Modeling Language User Guide, The*. [S.l.: s.n.], 2005. 496 p. ISBN 0321267974.

MORIARTY, K. et al. *PKCS #1: RSA Cryptography Specifications Version 2.2*. RFC Editor, 2016. RFC 8017. (Request for Comments, 8017). Disponível em: <https://rfc-editor.org/rfc/rfc8017.txt>.

KATZAND, J.; LINDELL, Y. *Introduction to Modern Cryptography*. [S.l.: s.n.], 2007. 406-407 p.

CHHETRI, N. A Comparative Analysis of Node . js (Server-Side JavaScript). *Culminating Projects in Computer Science and Information Technology*, p. 79, 2016.

Node.js Foundation. *Node.js*. 2018. Disponível em: <https://nodejs.org>.

FIELDING, R. T. *Architectural Styles and the Design of Network-based Software Architectures*. 76 p. Doctoral dissertation — University of California, 2000.