

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
SISTEMAS DE INFORMAÇÃO

Maurício de Vasconcelos Barros

**Um comprovante de vacinação baseado em Identidade Auto-Soberana, Blockchain e
Provas de Zero Conhecimento**

Florianópolis
2021

Maurício de Vasconcelos Barros

**Um comprovante de vacinação baseado em Identidade Auto-Soberana,
Blockchain e Provas de Zero Conhecimento**

Trabalho de Conclusão de Curso submetido ao Curso de Graduação em Sistemas de Informação do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito para obtenção do título de Bacharel em Sistema de Informação.

Orientador: Prof. Ricardo Felipe Custódio, Dr.

Coorientador: Prof. Frederico Schardong, Me.

Florianópolis

2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Barros, Maurício de Vasconcelos

Um comprovante de vacinação baseado em Identidade Auto
Soberana, Blockchain e provas de zero conhecimento /
Maurício de Vasconcelos Barros ; orientador, Ricardo Felipe
Custódio, coorientador, Frederico Schardong, 2021.

83 p.

Trabalho de Conclusão de Curso (graduação) -
Universidade Federal de Santa Catarina, Centro Tecnológico,
Graduação em Sistema de Informação, Florianópolis, 2021.

Inclui referências.

1. Sistema de Informação. 2. Identidade Digital. 3.
Identidade Auto-Soberana. 4. Blockchain. 5. Covid-19. I.
Felipe Custódio, Ricardo. II. Schardong, Frederico. III.
Universidade Federal de Santa Catarina. Graduação em
Sistema de Informação. IV. Título.

Maurício de Vasconcelos Barros

Um comprovante de vacinação baseado em Identidade Auto-Soberana, Blockchain e Provas de Zero Conhecimento

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Bacharel em Sistema de Informação e aprovado em sua forma final pelo curso de Graduação em Sistemas de Informação.

Florianópolis, 15 de Setembro de 2021.

Prof. Álvaro Junio Pereira Franco, Dr
Coordenador do Curso

Banca Examinadora:

Prof. Ricardo Felipe Custódio, Dr.
Orientador
Universidade Federal de Santa Catarina

Prof. Frederico Schardong , Me.
Coorientador
Instituto Federal do Rio Grande do Sul

Prof. Alexandre Augusto Giron, Me.
Avaliador
Universidade Tecnológica Federal do Paraná

Dedico esse trabalho às mulheres de minha vida, Ana e Karla,
que me ensinam todos os dias o que é amar incondicionalmente.

AGRADECIMENTOS

Agradeço a todos os companheiros e companheiras que participaram nessa jornada acadêmica. Aos meus familiares por sempre estarem presentes. Aos meus colegas de trabalho e faculdade, a todo o pessoal do LabSec, que tanto me ensinam. Aos meus orientadores por me guiarem nos caminhos da ciência, Ricardo Custódio, e em especial Frederico Schardong pela atenção e tutoria oferecida. Agradeço a todos os meus professores e coordenadores, a todo o pessoal da UFSC, de apoio e administrativo. E por fim, agradeço a todos aqueles que acreditam, lutam e contribuem para um universidade pública, gratuita e de qualidade.

RESUMO

A medida que a sociedade vai convergindo para o reino online, mais dados pessoais vão circulando pelas redes, trazendo preocupações de diferentes ordens: privacidade, segurança, propriedade dos dados. Novos mecanismos de gerenciamento desses dados fazem-se necessários. O estourar da pandemia de Covid-19 em 2020 ajudou a acelerar o processo de “virtualização” da sociedade, ampliando os horizontes do mundo online. O presente trabalho estuda esse problema fazendo uso do paradigma de Identidade Auto-Soberana, onde a arquitetura do sistema permite que o usuário seja o real proprietário de sua identidade e dos dados a ela associado. Para alcançar a compreensão desse novo modelo, primeiro é feita uma definição de uma série de conceitos basilares, ferramentas e tecnologias referentes ao tema, tais como Identidade Digital, Identidade Auto-Soberana, Credenciais Verificáveis, Blockchain, Hyperledger, entre outras. Após essa conceitualização, foi desenvolvido um protótipo de sistema que oferece credenciais verificáveis para serem usadas como um comprovante de vacinação. Tal comprovante utiliza técnicas de divulgação seletiva e provas de zero conhecimento, sendo capaz de informar apenas um subgrupo das informações contidas na credencial, promovendo maior segurança e privacidade dos dados contidos na credencial.

Palavras-chave: Identidade Digital, Identidade Auto-Soberana, Blockchain, Covid-19.

ABSTRACT

As society converges towards the online realm, more personal data circulates through the networks, bringing concerns of different orders: privacy, security, ownership of data. New mechanisms for managing this data are needed. The outbreak of the Covid-19 pandemic in 2020 has contributed to accelerate the process of “virtualization” of society, expanding the horizons of the online world. The present work studies this problem using the Self-Sovereign Identity paradigm, where the system architecture allows the user to be the real owner of his identity and the data associated with it. In order to understand this new model, a series of basic concepts, tools and technologies related to this work is defined, such as Digital Identity, Self-Sovereign Identity, Verifiable Credentials, Blockchain, Hyperledger, among others. After this conceptualization, a proposal and implementation of a system prototype that offers verifiable credentials to be used as proof of vaccination is carried out. Such proof uses selective disclosure techniques and proof of zero knowledge, being able to inform only a subgroup of the information contained in the credential, promoting greater security and privacy of the data contained in the credential.

Keywords: Digital Identity, Self-Sovereign Identity, Blockchain, Covid-19.

LISTA DE ILUSTRAÇÕES

Figura 1 – Modelo de Identidade Isolada.	21
Figura 2 – Modelo de Identidade Federada.	22
Figura 3 – Modelo de Identidade Auto-Soberana.	23
Figura 4 – Função Hash: A é o domínio e B é a imagem.	26
Figura 5 – Exemplo da estrutura de um DID.	27
Figura 6 – Estrutura de uma Declaração.	28
Figura 7 – Componentes básicos de uma Credencial Verificável.	29
Figura 8 – Arquitetura dos blocos na implementação de Nakamoto.	31
Figura 9 – Árvore de Hash ou Árvore Merkle.	33
Figura 10 – Hyperledger Indy é composto pelo Indy-Node e Indy-Plenum.	36
Figura 11 – Exemplo de escrita de esquema no Indy.	37
Figura 12 – Composição do Registro Distribuído Hyperledger Indy.	38
Figura 13 – Pool Ledger.	39
Figura 14 – Domain Ledger.	40
Figura 15 – Audit Ledger.	41
Figura 16 – Estrutura interna de um Agente Aries.	44
Figura 17 – Papeis envolvidos no sistema proposto	48
Figura 18 – Arquitetura do protótipo proposto.	49
Figura 19 – Telas do protótipo	52
Figura 20 – Conexão entre vacinador e vacinado.	53
Figura 21 – Emissão do comprovante de vacinação.	54
Figura 22 – O verificador se conecta ao portador da credencial.	55
Figura 23 – Requisição de provas	56
Figura 24 – Transação de emissão do DID do emissor vista no Indy Scan.	63
Figura 25 – Transação da emissão de esquema visto pelo Indy Scan.	63
Figura 26 – Transação da emissão de definição de credencial.	64

SUMÁRIO

1	INTRODUÇÃO	17
1.1	OBJETIVOS	18
1.1.1	Objetivos Gerais	18
1.1.2	Objetivos Específicos	18
1.2	ORGANIZAÇÃO	19
2	IDENTIDADES DIGITAIS	21
2.1	MODELO DE IDENTIDADE ISOLADA	21
2.2	MODELO DE IDENTIDADE FEDERADA	21
2.3	MODELO DE IDENTIDADE AUTO-SOBERANA	22
3	TERMINOLOGIA E CONCEITOS	25
3.1	RESUMOS CRIPTOGRÁFICOS (HASH)	25
3.2	CRIPTOGRAFIA ASSIMÉTRICA	26
3.3	ASSINATURA DIGITAIS	26
3.4	IDENTIFICADORES DESCENTRALIZADOS (DID)	27
3.5	CREDENCIAIS VERIFICÁVEIS	28
3.6	CARTEIRAS DIGITAIS	29
3.7	ESQUEMAS E DEFINIÇÃO DE CREDENCIAIS	29
3.8	PROVAS DE ZERO CONHECIMENTO	29
3.9	TECNOLOGIA BLOCKCHAIN	30
3.9.1	Árvore Merkle	32
3.9.2	Prova de Trabalho (<i>Proof of Work</i>)	32
3.9.3	Prova de Participação (<i>Proof of Stake</i>)	33
4	HYPERLEDGER INDY	35
4.1	INDY DISTRIBUTED LEDGER	35
4.2	CONJUNTO DE NODOS	36
4.3	REGISTRO DISTRIBUÍDO	38
4.4	TIPOS DE REGISTROS DISTRIBUÍDOS	38
4.4.1	Config Ledger	38
4.4.2	Pool Ledger	39
4.4.3	Domain Ledger	40
4.4.4	Audit Ledger	40
5	HYPERLEDGER ARIES	43
5.1	ARIES AGENT	43
5.2	DIDCOMM	43

6	PASSAPORTE COVID	47
7	IMPLEMENTAÇÃO	49
7.1	FERRAMENTAS UTILIZADAS	49
7.2	PROTÓTIPO	50
7.3	RESULTADOS	53
8	CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS	57
8.1	CONSIDERAÇÕES FINAIS	57
8.2	TRABALHOS FUTUROS	58
	REFERÊNCIAS	59
	APÊNDICE A – VISUALIZAÇÃO DAS TRANSAÇÕES	63
	APÊNDICE B – ARTIGO SBC	65

1 INTRODUÇÃO

Nas últimas décadas o número de dados pessoais que circulam online vem crescendo de forma vertiginosa. Boa parte desses dados partem da união das redes sociais com a internet móvel. Cada vez mais setores de nossas vidas são passadas online, processo acelerado em decorrência da pandemia de Covid-19, que colocou partes da população em formas de trabalho e ensino remoto. Cada vez mais aumentamos a estatura de nossas vidas digitais.

Essas novas possibilidades nos apresentam novos desafios. O processo súbito de “virtualização” desencadeado pela pandemia, muitas vezes não ofereceu tempo e/ou treinamento necessário para a mudança para a rotina online, e se por um lado estamos mais ágeis, mais conectados e mais dinâmicos, por outro lado também estamos mais vulneráveis.

Nesse contexto emerge uma discussão a respeito da privacidade desses dados de usuários. Grandes empresas que aglomeram dados de usuários, por vezes coletam e os utilizam de forma abusiva. Exemplo disto foi o caso em 2018 da Cambridge Analytica, onde os dados de mais de cinquenta milhões de usuários do Facebook foram obtidos sem permissão e utilizados para coordenar campanhas eleitorais baseadas em perfis psicológicos extraídos dos dados obtidos (ROSENBERG; CONFESSORE; CADWALLADR, 2018).

Exemplos dessa discussão são as recentes leis de proteção de dados que vem surgindo pelo mundo; a partir de 2020 entrou em vigor no Brasil a Lei Geral de Proteção de Dados (BRASIL, 2018). Nesse novo horizonte jurídico, o cidadão ganha mais garantias sobre seus dados.

Embora a ideia de “propriedade de dados” venha ganhando força como instituição jurídica, muito ainda se carece de uma estrutura que permita um gerenciamento e controle efetivo da imensidão de dados pessoais gerados na internet todos os dias.

Para que a sociedade possa se adequar a essas novas demandas sociais, políticas e jurídicas, novos mecanismos de gestão de dados serão necessários, e para superar tais obstáculos novas ideias e tecnologias de gerenciamento devem ser pensadas. Entre esses novos mecanismos estarão novas formas de se pensar as Identidades Digitais.

Esse processo de “virtualização” transferiu as identidades “clássicas” baseadas em papel, para uma versão digitalizada, que é chamada de identidade digital (YONG et al., 2011). O ISO 24760-1, que tem como tema segurança e privacidade para gerenciamento de identidade, coloca identidade digital como sendo “um conjunto de atributos relacionados a uma entidade”(ISO, 2019). Já em Maliki e Seigneur (2007) é definido que a identidade digital é a representação dessa entidade vinculada a um contexto específico.

Gestão de identidade é um processo para permitir a administração de uma identidade digital. Composta por políticas e tecnologias de forma a identificar entidades e permitir acesso a serviços (FERDOUS; CHOWDHURY; ALASSAFI, 2019). O sistema que permite essa gestão de identidade é chamado de Sistema de Gerenciamento de Identidades.

Os sistemas de gerenciamento atuais são frequentemente centralizados, com a propriedade dos dados pertencendo ao provedor de identidade, tirando das mãos dos usuários a

manutenção de seus dados e identidades digitais.

Identidade Auto-Soberana é um modelo de identidade digital. Segundo Allen (2016), em um sistema de Identidade Auto-Soberana o usuário deve ser central na administração da identidade, com o verdadeiro controle daquela identidade digital.

O conceito de Identidade Auto-Soberana é relevante em casos onde os dados pessoais possuem grande sensibilidade, como são os dados de saúde. Dados de pacientes são sensíveis, e exigem um cuidado especial em seu armazenamento, tratamento e compartilhamento.

Durante a pandemia de Covid-19, surgiram iniciativas de compartilhamentos de dados anonimizados que contribuam para a pesquisa do tema. Exemplos dessas iniciativas são o COVID DataSharing/BR (FAPESP, 2020) no Brasil, e o United States' National Covid Cohort Collaborative (N3C) (NCATS, 2021), nos Estados Unidos.

Compartilhar dados de prontuários de forma anonimizada, torna possível a compilação de um grande número de dados, amparando as políticas públicas de saúde, melhorando a tomada de decisão. Utilizar técnicas de divulgação seletiva permite respeitar a privacidade dos pacientes

O trabalho proposto busca investigar a tecnologia usada em sistemas de Identidade Auto-Soberana, escolhendo como caso de uso para implementação de um protótipo, a emissão e verificação de um comprovante de vacinação.

Usando um conjunto de ferramentas como o Hyperledger Indy, Aries e Ursa, foi possível montar uma prove de conceito de um comprovante de vacinação em formato de uma credencial verificável que permite provas de zero conhecimento e divulgação seletiva.

Tal comprovante permite ao paciente comprovar sua vacinação sem expor nenhum dado pessoal, mostrando apenas uma prova de zero conhecimento que atesta sua vacinação, tornando o processo menos invasivo.

1.1 OBJETIVOS

1.1.1 Objetivos Gerais

O objetivo do trabalho é realizar um estudo sobre o conceito e as tecnologias envolvidas no paradigma de Identidade Auto-Soberana, buscando compreender seu funcionamento.

1.1.2 Objetivos Específicos

Os objetivos específicos são:

- Pesquisar as tecnologias e conceitos que permitam uma credencial em Identidade Auto-Soberana.
- Modelar um sistema de credenciais Auto-Soberanas com as tecnologias estudadas.

- Implementar uma prova de conceito de comprovante de vacinação por meio de uma credencial Auto-Soberana que possua divulgação seletiva e provas de zero conhecimento.

1.2 ORGANIZAÇÃO

Em um primeiro momento é apresentado conceitos chaves que serão tratados, como identidades digitais e Auto-Soberana. Em seguida o trabalho perpassa diversos temas pertinentes à tecnologia abordada, como funções Hash, credenciais verificáveis, DIDs, entre outros. Na sequência são abordadas as tecnologias e ferramentas descobertas, como Blockchain e os projetos Hyperledger. Por fim, é exposto a proposta e implementação realizada no presente estudo.

2 IDENTIDADES DIGITAIS

O gerenciamento de identidades digitais vem se modificando constantemente conforme a internet e suas tecnologias vão avançando e ganhando maior importância e criticalidade. A seguir o trabalho pontua alguns desses principais modelos de gerenciamento de identidades.

2.1 MODELO DE IDENTIDADE ISOLADA

O modelo de identidade isolada foi o primeiro modelo, sendo o mais simples (FERDOUS; CHOWDHURY; ALASSAFI, 2019), representado na Figura 1. Nesse arranjo o provedor de serviços (SP - Service Provider) funcionaria também como provedor de identidade (IdP – Identity Provider). Neste modelo apenas existe o usuário e o provedor de serviço. Cada web-service que oferece algum serviço que requer autenticação, deveria implementar seu próprio sistema de gerenciamento e acesso de identidades.

O resultado deste modelo foi que os usuários tinham muitas identidades digitais espalhadas pelos diversos serviços online. Além disso, cada provedor de serviços online (web-services) tinha que arcar com os custos e dificuldades de implementação e manutenção de um sistema de gerenciamento de identidades, o que envolve a proteção contra possíveis ataques e vulnerabilidades.

Figura 1 – Modelo de Identidade Isolada.



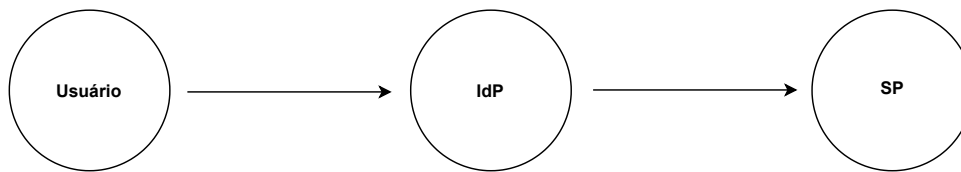
Fonte – Inspirado em Schardong e Custódio (2021)

2.2 MODELO DE IDENTIDADE FEDERADA

No modelo federado cada Domínio de Identidade consiste de um provedor de identidade com um ou mais provedores de serviços (ALLEN, 2016). O provedor de serviço utiliza o provedor de identidade para autenticação, identificação, registro e remoção de usuários. O arranjo alcançado, como exposto pela Figura 2, é uma federação onde em um provedor de identidade, após identificado, o usuário pode acessar qualquer provedor de serviços que compartilhe daquele mesmo provedor de identidade (FERDOUS; CHOWDHURY; ALASSAFI, 2019).

Neste modelo os usuários não precisam possuir diversas identidades diferentes e os provedores de serviço não precisam implementar sua própria estrutura de gerenciamento de identidade. Porém o modelo federado gerou consequências não esperadas, com uma concentração imensa de dados nas mãos de poucos provedores de identidade, como Facebook, Google,

Figura 2 – Modelo de Identidade Federada.



Fonte – Inspirado em Ferdous, Chowdhury e Alassafi (2019)

Twitter e etc. Essas empresas se tornaram imensos silos de dados, se convertendo em verdadeiras “oligarquias” de provedores de identidade (SCHARDONG; CUSTÓDIO, 2021).

Por concentrar um número muito alto de dados, esses silos se tornaram centros de atenção, chamarizes de ataques. Além disso questões como vazamentos de dados, segurança e privacidade iniciam a emergir no horizonte das questões sobre identidades digitais. Esses dados são sobre os usuários, porém os usuários não possuem esses dados; os usuários não possuem suas identidades digitais. Não somos capazes de exercer a propriedade de nossos dados.

2.3 MODELO DE IDENTIDADE AUTO-SOBERANA

A discussão sobre identidade auto-soberana inicia com a ideia que o usuário deveria possuir seus dados, possuir sua identidade digital. Embora a definição de Identidade Auto-Soberana ainda esteja em aberto, como visto em Schardong e Custódio (2021), Mühle et al. (2018) e Ferdous, Chowdhury e Alassafi (2019), em um modelo de identidade auto-soberana o usuário deve ser o soberano perante sua identidade, possuindo total controle. Os dados de identidade podem ser armazenados localmente, com os usuários, que apresentam esses dados quando necessário.

Em 2016, um texto em um blog escrito por Christopher Allen, propôs 10 princípios para identidades auto-soberanas (ALLEN, 2016), e embora se trate de um texto de blog, foi usado como guia e referências de diversos trabalhos que se propuseram a trabalhar com Identidade Auto-Soberana, como em Mühle et al. (2018), Ferdous, Chowdhury e Alassafi (2019), Kim et al. (2021), Bokkem et al. (2019), Schardong e Custódio (2021) entre outros.

Os dez princípios propostos por Allen são: (1) Existência – O usuário deve existir independente de qualquer provedor de serviço/provedor de identidade. (2) Controle – O usuário deve controlar suas identidades. (3) Acesso – O usuário deve sempre ter acesso a seus dados. (4) Transparência – Todos os sistemas e algoritmos devem ser transparentes para o usuário. (5) Persistência – As identidades devem ser persistidas. (6) Portabilidade – Os serviços e informações sobre a identidade do usuário deve ser transportável. (7) Interoperabilidade – As identidades devem possuir o maior alcance de uso possível entre diferentes sistemas. (8) Consentimento – O usuário sempre precisa dar seu consentimento para o uso de seus dados de identidade. (9) Minimização – Quando necessário mostrar alguma informação, sempre mostrar o mínimo possível para a realização da tarefa. (10) Proteção – Os direitos dos usuários devem ser protegidos.

Uma possível forma de implementar um sistema de gerenciamento de identidades Auto-Soberanas é com o auxílio da tecnologia Blockchain. Dessa forma, o usuário apresenta sua credencial e a parte verificadora confere no registro Blockchain sua autenticidade, como mostrado na Figura 3. Embora seja possível implementar uma Identidade Auto-Soberana sem o uso da tecnologia Blockchain, como afirma Bokkem et al. (2019), a tecnologia Blockchain é uma excelente fundação na qual é possível montar uma Identidade Auto-Soberana. Para deixar informações disponíveis de maneira pública, como esquemas de credenciais, esquemas de revogação, DID's públicos ou chaves públicas, Blockchain funciona adequadamente, diminuindo a necessidade de pontos centralizadores.

Figura 3 – Modelo de Identidade Auto-Soberana.



Fonte – Inspirado em Naik e Jenkins (2020)

3 TERMINOLOGIA E CONCEITOS

De forma a melhor explicar o protótipo e a abordagem utilizada no estudo, faz-se necessário uma introdução a respeito de conceitos basilares: blockchain e as partes que o compõem como hashes criptográficos e árvores de hash. Mecanismos utilizados em implementações de identidades descentralizadas como DIDs e credenciais verificáveis entre outros.

3.1 RESUMOS CRIPTOGRÁFICOS (HASH)

Resumos criptográficos, ou funções de Hash, possuem papel de importância na criptografia. Um dos principais usos da função Hash é para prover integridade ao dado. Sendo uma função, ela possui a característica de cada elemento em seu domínio ser mapeado até um elemento em sua imagem, além de ser unidirecional.

Como visto na Figura 4, todos os elementos em A (domínio) são mapeados até um único elemento em B (imagem) por meio de uma função (f). Em uma função de Hash, o A (domínio) seria o conjunto de todas as sequências possíveis de bits, ou seja, potencialmente infinito, enquanto o B (imagem) seria o conjunto de todas as sequências de tamanho n-bits onde $n > 0$, como mostrado na Tabela 1, onde a imagem da função é de tamanho de 256 bits.

A função de Hash cria uma "digital" da sequência de dados, assim qualquer mudança nos dados pode ser percebida, pois gera um resumo criptográfico diferente. Da mesma forma, se a sequência de dados permanecer a mesma, a saída da função de Hash será a mesma, garantindo integridade. Como a saída da função tem um tamanho fixo e relativamente pequeno, é possível verificar de forma simples a integridade de arquivos imensos.

As funções Hash possuem três características principais: resistência a pré-imagem, resistência a segunda pré-imagem, e resistência a colisão (YAGA et al., 2018):

A resistência a pré-imagem garante que a função seja unidirecional, que vá apenas na direção do domínio para a imagem, e que seja computacionalmente inviável fazer o caminho inverso.

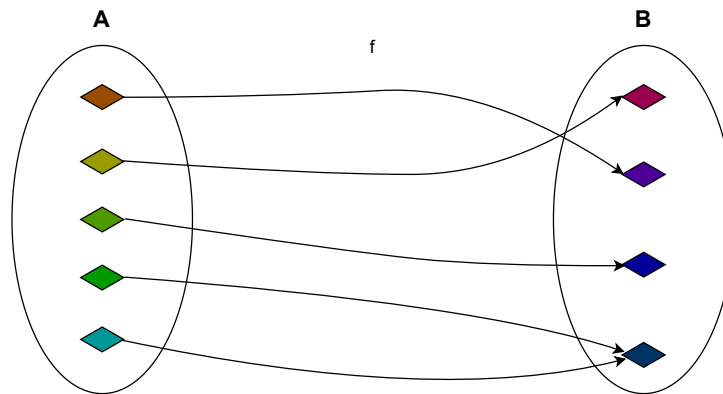
Já a resistência a segunda pré-imagem garante que seja computacionalmente inviável encontrar um segundo elemento no domínio ao qual o hash irá ser um valor específico (conhecido) na imagem. Ou seja, inviável encontrar um segundo elemento no domínio que produza um mesmo elemento na imagem.

E por fim a resistência a colisão garante que seja computacionalmente inviável encontrar dois elementos no domínio que produzam um mesmo elemento na imagem (YAGA et al., 2018).

Entre os diversos algoritmos de hash, como MD4, MD5, SHA-1, SHA512, a função hash frequentemente utilizada em implementações de Blockchain é o algoritmo Secure Hash Algorithm de tamanho 256 bits (YAGA et al., 2018), ou SHA-256.

As funções hash são utilizadas na blockchain como uma forma rápida de verificação de integridade.

Figura 4 – Função Hash: A é o domínio e B é a imagem.



Fonte – O autor.

Tabela 1 – Exemplos de Domínio e Imagem de uma função hash SHA-256

Domínio	Imagem
Olá, mundo!	9583b013baa520d3a893c4270d0c67732d7ef1768eb0a13533b4e7b134d4b131
1	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
Função hash.	3917927e448b2f8b167bfe6c7d9bbd97f7f9b88afd9a7c35073b2560ba3f5577

3.2 CRIPTOGRAFIA ASSIMÉTRICA

Na criptografia de chaves assimétricas, duas chaves relacionadas são utilizadas. Uma é a chave pública e a outra é a chave privada. Com essas duas chaves é possível realizar operações criptográficas complementares, como encriptar e decriptar, ou assinar e verificar (STALLINGS, 2015). Portanto, tudo o que for cifrado pela chave privada poderá ser decifrado pela chave pública, e vice-versa. Esse par de chaves deve possuir a característica de ser computacionalmente inviável obter a chave privada a partir da chave pública.

Para que o criptossistema de chave pública opere de forma segura, a chave privada deve sempre manter-se privada, adequadamente armazenada e protegida. Caso uma mensagem seja cifrada utilizando a chave pública, apenas quem possui a chave privada será capaz de decifrar. Por outro lado, se a mensagem foi cifrada com a chave privada, todos aqueles que possuem a chave pública poderão decifrar, porém com a certeza de que a mensagem pertence ao dono da chave privada.

3.3 ASSINATURA DIGITAIS

Assinaturas Digitais fornecem não-repúdio, autenticidade e integridade às mensagens, dados ou documentos assinados (STALLINGS, 2015). A assinatura é baseada em funções Hash e criptografia assimétrica.

Um Certificado Digital associa uma chave pública a uma identidade (STALLINGS,

2015) por meio de um documento que é assinado digitalmente por uma Autoridade Certificadora, entidade responsável por emitir os certificados digitais.

Para que o sistema de assinatura digital baseado em chaves assimétricas funcione com validade jurídica, é necessário uma infraestrutura de chave pública (representada no Brasil pela ICP Brasil (ITI, 2021)), composta por diversos processos, políticas, serviços e atores com o objetivo de gerenciar, distribuir, armazenar e revogar os certificados digitais. Essa infraestrutura de chaves públicas tem como objetivo primário, tornar possível a aquisição segura e eficiente de chaves públicas (STALLINGS, 2015).

Em uma assinatura digital o valor de hash da mensagem (dado ou documento) é encriptado com a chave privada do assinante. Conhecendo a chave pública desse assinante, por meio de (por exemplo) um Certificado Digital, é possível decriptar o texto cifrado, obtendo assim o hash original da mensagem, provendo tanto autenticidade como integridade. Autenticidade por meio da encriptação com a chave privada e integridade por meio da checagem do resumo criptográfico (Hash).

Portanto a assinatura (geralmente) é composta de dois processos: Primeiro tira-se o resumo criptográfico do documento ou mensagem, e em seguida encripta-se aquele resumo criptográfico. Assim, o que é assinado é o hash da mensagem, dado ou documento, e não a mensagem, dado ou documento original. Dessa forma a assinatura fica de um tamanho fixo e reduzido, economizando poder computacional de encriptação e decriptação.

3.4 IDENTIFICADORES DESCENTRALIZADOS (DID)

Um Identificador Descentralizado, ou DID, é uma referência global única ligada a um documento DID. Seu formato é uma sequência textual composta por três partes: <esquema DID>:<método DID>:<Identificador específico> (SPORNY et al., 2021) como apresentado na Figura 5. São tipos de identificadores que permitem identidades digitais descentralizadas.

Figura 5 – Exemplo da estrutura de um DID.



Fonte – Sporny et al. (2021).

DIDs foram projetados para operar de forma independente de registros centralizados, provedores de identidades e autoridades certificadoras. Uma mesma entidade pode possuir diversos DIDs, um para cada relacionamento com outra entidade.

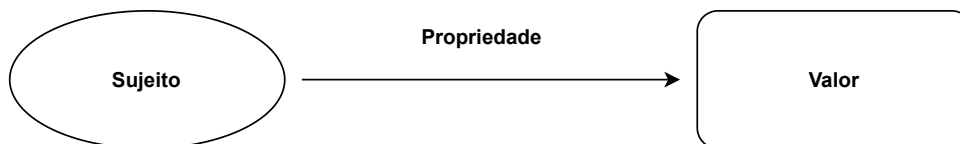
Todo DID é ligado a um documento DID, que é um conjunto de dados em JSON que descreve uma entidade, especificando chaves públicas, *endpoints* de serviços, etc. Essa entidade pode ser uma pessoa, um grupo, uma organização, um objeto Internet das Coisas (SPORNY et al., 2021). Todo DID é associado a uma chave verificadora.

Em um exemplo de caso de uso, um usuário acessa um site provedor de serviço e se registra, criando e enviando um novo DID nunca utilizado. O provedor de serviço por sua vez também cria e envia um DID novo. Esses dois DIDs representam o relacionamento do usuário com o provedor de serviço. Agora, para que os dois se comuniquem, eles possuem um *endpoint* (contido do documento DID) e uma chave pública para mensagens encriptadas ponto-a-ponto. Quando o usuário retornar ao provedor de serviço, ambos trocam mensagens encriptadas e confirmam se o outro possui a chave privada para decriptar a mensagem.

3.5 CREDENCIAIS VERIFICÁVEIS

Uma credencial é um conjunto de uma ou mais declarações (claims) que são feitas pela mesma entidade Emissora. Emissores fazem as afirmações em uma declaração e emitem as credenciais. Declarações (claims) são afirmações a respeito de um “sujeito”, sendo esse sujeito algo ao qual uma declaração possa ser feita. São expressas em uma relação sujeito-propriedade-valor (SPORNY; LONGLEY; CHADWICK, 2019), como exposto na Figura 6.

Figura 6 – Estrutura de uma Declaração.



Fonte – Inspirado em Sporny, Longley e Chadwick (2019).

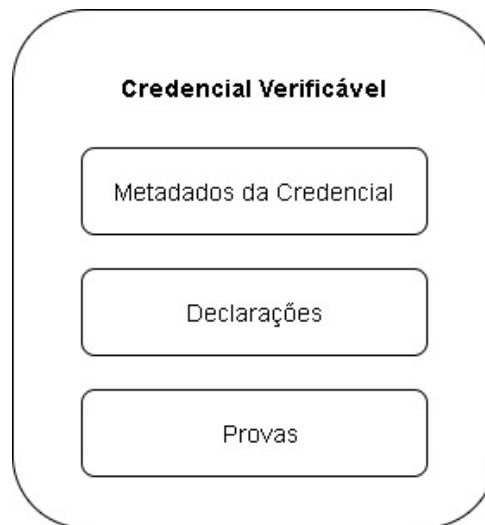
Credenciais podem ter metadados que descrevem propriedades como o emissor, data de validade, chave pública, revogação, etc. Credencial Verificável é um conjunto de declarações e metadados que podem provar criptograficamente o emissor por meio de uma assinatura digital (SPORNY; LONGLEY; CHADWICK, 2019), provendo integridade, autenticidade e não-repúdio, como representado na Figura 7.

Uma Apresentação é criada para mostrar declarações para um verificador. Um verificador é o papel de quem recebe uma Credencial Verificável para verificação. Essas Apresentações Verificáveis permitem apresentar apenas um subgrupo dos atributos.

Alguns arranjos de provas de Zero Conhecimento podem criar Apresentações que provam de forma indireta a posse de uma Declaração sem revelar o dado original (SPORNY; LONGLEY; CHADWICK, 2019).

Embora dois conceitos independentes, as Credenciais Verificáveis podem ser associadas a um DID por meio de um documento DID de forma a identificar um sujeito.

Figura 7 – Componentes básicos de uma Credencial Verificável.



Fonte – Inspirado em Sporny, Longley e Chadwick (2019).

3.6 CARTEIRAS DIGITAIS

Dentro do contexto da Identidade Auto-Soberana, uma Carteira Digital é um software onde ficam armazenadas as Credenciais Verificáveis, chaves de verificação e outros dados criptográficos. O software provê agentes para lidar com os relacionamentos criados pela carteira (KIM et al., 2021). Uma carteira digital baseia-se no modelo de chaves públicas, sendo a carteira a peça de software responsável por manter a chave privada protegida.

3.7 ESQUEMAS E DEFINIÇÃO DE CREDENCIAIS

Esquemas de credenciais são úteis para especificar a estrutura de uma coleção de dados. Esses esquemas são usados para confirmar que o conteúdo e a estrutura de uma credencial verificável estão em conformidade com o modelo esperado (SPORNY; LONGLEY; CHADWICK, 2019). Uma definição de credencial associa um esquema de credencial a um DID (do emissor). O emissor especifica uma definição de credencial que aponta para algum arquivo que representando um esquema (como um JSON), e deve ser usado pelo verificador para verificar se a credencial verificável está com a estrutura adequada.

3.8 PROVAS DE ZERO CONHECIMENTO

Provas de zero conhecimento, ou *Zero Knowledge Proof* (ZKP) em inglês, é um protocolo criptográfico onde um usuário é capaz de provar a outro usuário, através de computação polinomial, que ele conhece o valor de X, sem revelar qualquer outra informação além do fato que ele conhece X (HARIKRISHNAN; LAKSHMY, 2019). O resultado possível de uma prova de zero conhecimento é apenas aceitar ou rejeitar.

Zero Conhecimento é um sistema de prova interativo com dois atores, o Provedor P e o Verificador V . O Provedor é o ator que apresenta a prova, e o Verificador é aquele que a verifica. P e V devem compartilhar uma mesma entrada z , tal $(P, V)(z)$. Com essa entrada comum, P e V abrem um canal de comunicação e trocam uma sequência de mensagens, de forma que ao fim da interação o resultado deve ser $(P, V)(z) \{aceitar, rejeitar\}$ (IBRAHEM, 2012).

Segundo Qi e Chen (2009), um protocolo de prova pode ser considerado de zero conhecimento se possuir essas três características:

Completeness (*Completeness*): Considerando um verificador e um provedor honesto - após o cálculo da prova, se o resultado for verdadeiro, aquele que verifica pode aceitar a prova com probabilidade esmagadora de estar correto.

Eficácia (*Effectiveness*): Considerando um verificador e um provedor honesto - após o cálculo da prova, se o resultado for falso, aquele que verifica pode rejeitar a prova com probabilidade esmagadora de estar correto.

Zero Conhecimento: Considerando um verificador e um provedor honesto - após a verificação da prova, tendo sido a conclusão verdadeira, e estando o protocolo funcionando adequadamente, o verificador deve aceitar essa prova sem qualquer informação adicional.

Provas de Zero Conhecimento não são provas no sentido absoluto do termo, pois existe uma mínima probabilidade de um Provedor malicioso provar para um Verificador alguma declaração que seja falsa (IBRAHEM, 2012). Os protocolos de zero conhecimento são pensados de forma a utilizarem técnicas para a minimização dessa probabilidade de falha da prova.

3.9 TECNOLOGIA BLOCKCHAIN

A tecnologia Blockchain permite o fim da Confiança baseada em uma autoridade central, transitando para a Confiança distribuída baseada no protocolo Blockchain; os usuários são capazes de gerenciar seus dados através de “carteiras digitais”. As carteiras digitais são peças de software com o propósito (entre outros) de armazenar conteúdos criptográficos.

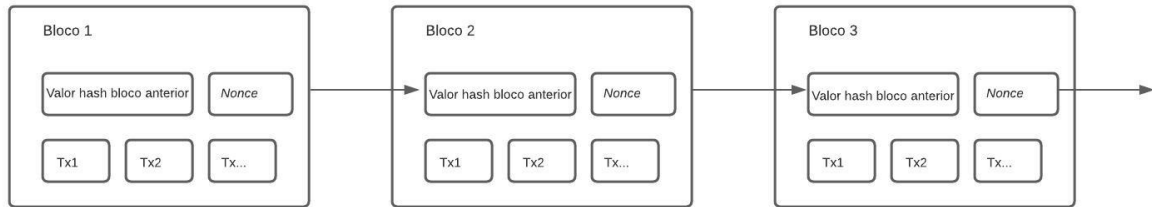
Nakamoto propôs em 2008 em seu artigo o Bitcoin (NAKAMOTO, 2008), um dinheiro eletrônico que poderia ser usado de forma peer-to-peer (P2P). Nakamoto argumenta que todo o comércio da internet baseia-se quase exclusivamente nas grandes instituições financeiras como fonte de Confiança, e propõe uma solução utilizando um servidor de timestamp distribuído peer-to-peer que é capaz de gerar provas computacionais da ordem cronológica das transações. Esse sistema utiliza o mecanismo de Proof of Work (PoW) e oferece uma proposta para resolver a vulnerabilidade do gasto-duplo (double-spending).

Essa solução ficou conhecida como Blockchain (cadeia de blocos), devido a sua estrutura de dados formada por uma lista interligada de blocos, onde cada bloco consiste de um conjunto de transações, o valor de hash do bloco anterior e um nonce, como mostrado na Figura 8.

Nessa implementação as duas estruturas principais são uma lista encadeada de hashes e uma árvore de hashes. A lista serve para manter história das transações, enquanto a árvore

serve para verificação de integridade.

Figura 8 – Arquitetura dos blocos na implementação de Nakamoto.



Fonte – Inspirado em Nakamoto (2008).

Nem todas as implementações de Blockchain possuem essa estrutura de dados de lista interligada, dessa forma o melhor termo a ser chamado seria Tecnologia de Registro Distribuído, ou em inglês Distributed Ledger Technology (DLT). Na bibliografia estudada os termos Blockchain e Registro Distribuído são em geral, intercambiáveis.

Esse Registro é distribuído e armazenado nos diferentes nodos em uma rede peer-to-peer (P2P), assim a segurança, imutabilidade e integridade dos dados é assegurada de forma descentralizada. Em geral, cada bloco é adicionado em um intervalo pré-definido, por meio de um algoritmo de consenso entre os nodos da rede. Esse algoritmo de consenso aliado à estrutura de hashes criptográficos, são peças-chaves para garantir a integridade dos dados.

A Tecnologia de Registro Distribuído oferece um grande potencial de casos de uso e vem ganhando muita atenção ultimamente e prometendo transformações em diferentes domínios (FERDOUS; CHOWDHURY; ALASSAFI, 2019). Novas formas de implementação surgiram após a implementação inicial de Nakamoto, trazendo novas possibilidades, melhor escalabilidade, maior eficiência energética, além da introdução (pela Ethereum) de smart-contracts ou contratos inteligentes, que são programas de computador (linhas de código) operando no Registro Distribuído, permitindo a operação de contratos de forma semi-automatizada.

As redes Blockchain podem ser do tipo público ou privado quanto à validação. No tipo público (ou *permissionless*) qualquer pessoa pode se juntar à rede e participar do processamento de consenso e validação dos blocos. Já no tipo privado (ou *permissioned*) apenas os nodos autorizados podem participar do processo de validação dos blocos (YAGA et al., 2018).

As redes públicas são registros descentralizados abertos a todos. Frequentemente são software livre, de desenvolvimento aberto e compartilhado. Como a rede é aberta para todos enviarem transações e escreverem novos blocos, a leitura desses blocos também é aberta para todos, fazendo essas blockchains serem também públicas no que diz respeito ao acesso – qualquer um pode ler o registro.

Como qualquer pessoa pode escrever e ler blocos na blockchain pública, é necessário um mecanismo de consenso que previna ataques maliciosos, muitas vezes exigindo consumo de algum recurso. Podemos citar como exemplos desses protocolos de consenso o prova de trabalho (*proof of work*) e o prova de participação (*proof of stake*).

Por outro lado as redes privadas necessitam da autorização de algum tipo de autoridade, seja ela central ou descentralizada, para a escrita dos blocos. Também é possível restringir o envio de transações e a leitura dos dados, tornando-a privada quanto ao tipo de acesso.

As redes privadas também utilizam algum mecanismo de consenso, porém geralmente não necessitam de alto consumo de recursos. Como as redes privadas exigem algum tipo de identificação para a participação, existe um nível maior de confiança entre os participantes. Caso algum participante seja identificado como malicioso seu acesso pode ser revogado da rede. Assim os modelos de consenso utilizados em redes privadas são mais rápidos e mais energeticamente eficientes (YAGA et al., 2018). Um exemplo de consenso que pode ser utilizado nessas redes é o protocolo RBFT (*Redundant Byzantine Fault Tolerance*).

3.9.1 Árvore Merkle

O cabeçalho dos blocos da blockchain são compostos por quatro componentes, um carimbo de tempo, um número aleatório (nonce), uma referência ao hash do bloco anterior e um lista de todas as transações contidas naquele bloco (LIM et al., 2018). Essa lista de todas as transações do bloco é armazenada na forma de uma estrutura de dados chamada árvore de Merkle.

Árvore Merkle é uma árvore de hash. Tudo que se encontra dentro de uma árvore de Merkle são valores de hash. Trata-se de uma árvore binária (LIM et al., 2018), caso alguma folha esteja sozinha, seu valor é duplicado para retornar à estrutura binária, e assim ser possível calcular a árvore.

Uma árvore de hash é calculada das folhas para a raiz, cada nodo pai é composto pelo hash da concatenação dos dois nodos filhos. Assim, no exemplo da Figura 9, o nodo h9 é composto pelo hash da concatenação dos valores de seus dois nodos filhos h1 e h2. O nodo h13 é composto pelo hash da concatenação dos valores de seus dois nodos filhos h9 e h10. E por fim o nodo Raiz é composto pelo hash da concatenação dos valores de seus dois nodos filhos h13 e h14.

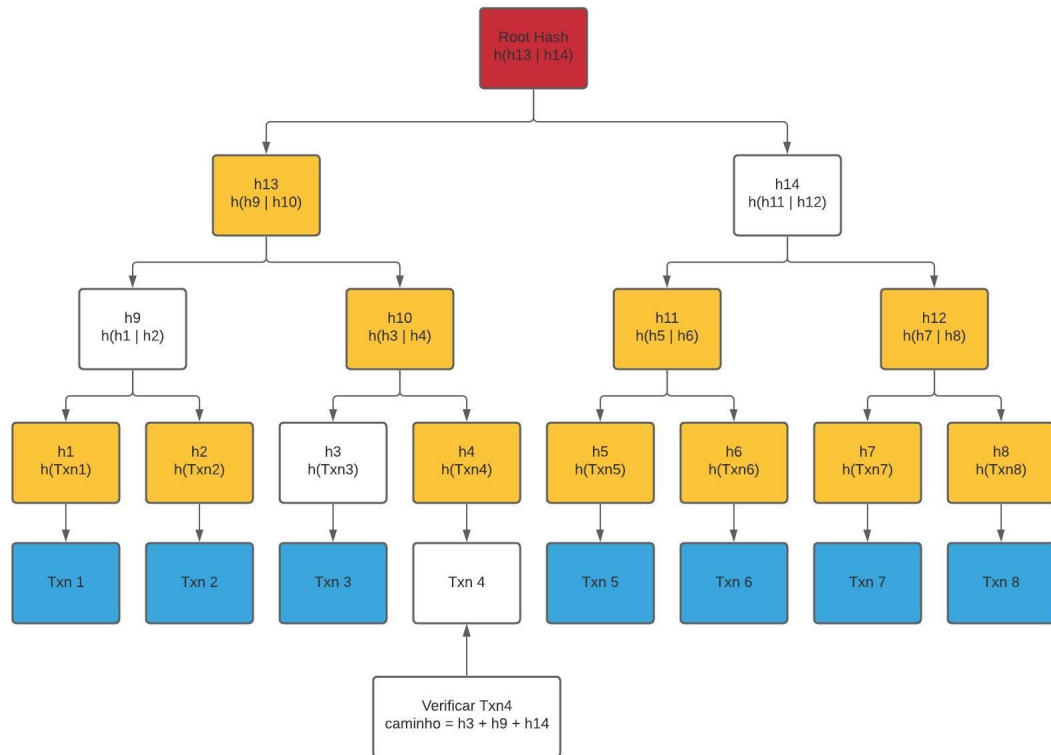
A árvore Merkle permite verificar se uma transação específica pertence a uma determinada Árvore Merkle sem precisar baixar todas as transações, sendo então uma forma rápida de verificar transações.

3.9.2 Prova de Trabalho (*Proof of Work*)

Esse algoritmo é o mais antigo e também um dos mais usados na tecnologia blockchain (LIM et al., 2018). Possui alto gasto energético.

No protocolo de consenso prova de trabalho, diversos usuários “disputam” a resolução de um “quebra-cabeça” matemático que é computacionalmente exigente. O primeiro usuário que solucionar o quebra-cabeça será aquele que publicará o próximo bloco, e com isso receberá uma recompensa.

Figura 9 – Árvore de Hash ou Árvore Merkle.



Fonte – Inspirado em Lim et al. (2018)

Em grandes redes que usam prova de trabalho, como a rede do Bitcoin, a forma de solucionar esse “quebra-cabeça” é executando a função hash seguidas vezes no cabeçalho do bloco, modificando apenas o nonce, e buscando um resultado de hash que seja menor que um valor previamente especificado (YAGA et al., 2018). Esse processo de executar a função hash diversas vezes, por tentativa e erro, é um processo que exige tanto capacidade computacional como energética.

O alvo buscado pode ser modificado de tempos em tempos para que haja um ajuste na dificuldade, como é o caso da rede Bitcoin (NAKAMOTO, 2008). Nesse protocolo, contanto que a maioria do poder computacional seja controlado por nodos honestos, o protocolo deverá funcionar adequadamente.

Assim que algum nodo resolve o quebra-cabeça, ele envia o bloco, junto com o nonce válido para os outros nodos da rede. Os nodos que o recebem, verificam se esse novo bloco corresponde ao quebra-cabeça, e se sim, o adicionam à sua cópia da Blockchain.

3.9.3 Prova de Participação (*Proof of Stake*)

No protocolo de prova de participação não existe a necessidade de solucionar os difíceis problemas matemáticos do protocolo prova de trabalho, o que diminui o gasto de recursos. A lógica da confiança nesse algoritmo é baseado na ideia de que quanto mais participação um

nodo possui, mais ele vai ter interesse que o sistema opere normalmente (YAGA et al., 2018). Essa “participação” é geralmente uma quantidade de cripto moeda que o dono do nodo colocou no sistema. O sistema realiza uma espécie de sorteio, onde sua chance de ganhar é proporcional ao tamanho de sua participação.

Na lógica desse sistema não é necessário a criação de novas moedas como recompensa. É possível que todas as moedas já estejam criadas. A recompensa é composta pelas taxas de transação.

4 HYPERLEDGER INDY

Hyperledger Indy é um projeto pertencente à comunidade Hyperledger. Hyperledger é uma comunidade open-source que tem por objetivo desenvolver frameworks, ferramentas e bibliotecas para permitir a implementação de Blockchains de nível empresarial (LINUX FOUNDATION, 2015). É uma colaboração global liderada pela Linux Foundation e inclui diversas empresas de tecnologias. Conta com diversas implementações de Blockchain para diferentes contextos.

Entre um dos projetos do Hyperledger há o HyperLedger Indy que oferece um ecossistema para gerenciamento de Identidade Auto-Soberana baseado em Blockchain (HYPERLEDGER, 2015).

4.1 INDY DISTRIBUTED LEDGER

O Registro Distribuído Indy é formado por dois projetos: Indy-Node e Indy-Plenum, como mostrado na Figura 10. Indy-Plenum é um Registro Distribuído de propósito geral, onde fica implementado o algoritmo de consenso, já o Indy-Node é uma especialização do Indy-Plenum, onde são implementadas as transações específicas relacionadas a identidade (SHCHERBAKOV, 2019).

O Hyperledger Indy possui o propósito de ser um Registro Distribuído específico para gerenciamento de identidade. Porém ele pode ser utilizado como um Registro de propósito geral.

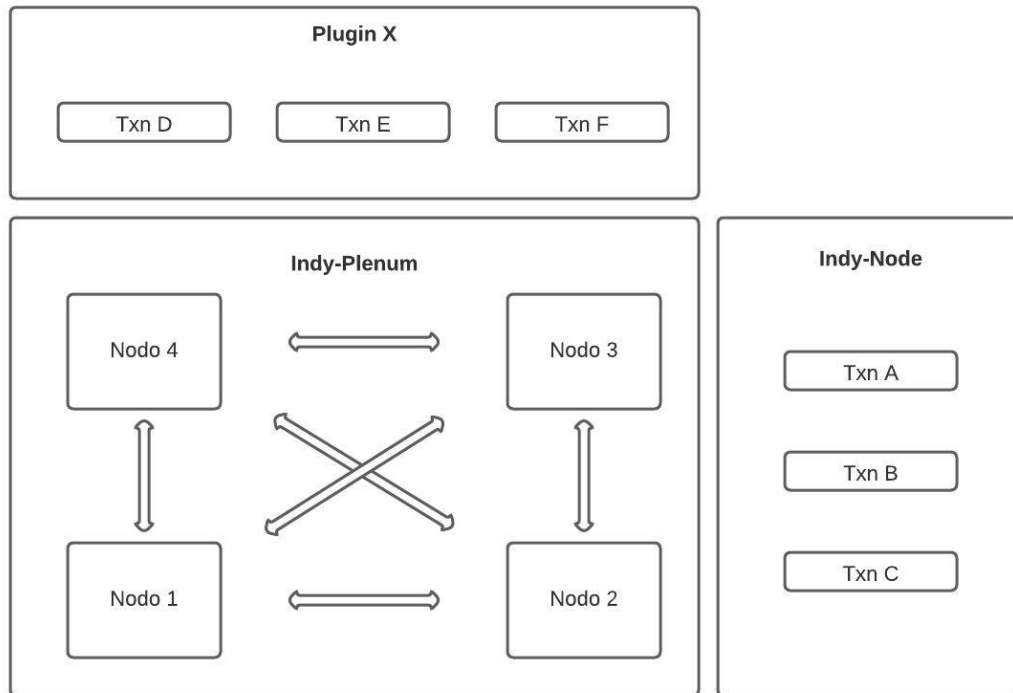
O Indy-Plenum é o núcleo central onde está implementado o algoritmo de consenso, é quem escreve no Registro. O Indy-Plenum pode ser estendido através de plugins onde são implementados transações personalizadas. É o que Indy-Node faz, implementa um plugin no Indy-Plenum que adiciona as transações específicas para o gerenciamento de identidade (como na Figura 10). Assim, da mesma forma é possível adicionar novos plugins para estender o Hyperledger Indy fazendo-o um Registro de propósito geral (SHCHERBAKOV, 2019).

O Registro Distribuído do HyperLedger Indy é do tipo público permissionado (HYPERLEDGER, 2018a). Permissionado na validação pois é necessário uma permissão (um papel específico na rede) para participar da validação das transações e para escrita. E publico pois o acesso à leitura é aberto.

Nenhum dado privado é escrito na Blockchain. São escritos apenas DID's públicos, chaves públicas, esquemas de credenciais e informações sobre revogações, garantindo assim a privacidade dos dados.

As requisições de escrita necessitam de Autenticação. Toda a Autenticação é baseada em informações contidas no próprio Registro (SHCHERBAKOV, 2019). As requisições de escrita devem ser assinadas digitalmente e essa assinatura é verificada com uma chave pública armazenada no Registro Distribuído. Requisições de leitura não necessitam nenhum tipo de Autenticação (acesso público).

Figura 10 – Hyperledger Indy é composto pelo Indy-Node e Indy-Plenum.



Fonte – Inspirado em Shcherbakov (2019).

A Autorização é baseada em papéis (roles) na rede (certos papéis são autorizados a fazer certas coisas), e também é dependente das informações contidas no Registro. Para requisições de leitura nenhuma Autorização é necessária (acesso público).

4.2 CONJUNTO DE NODOS

Sendo um Registro Distribuído, trata-se de uma aplicação distribuída, que utiliza um conjunto de nodos para operar (*node pool* em inglês). Existem dois conjuntos de nodos na implementação do Hyperledger Indy, sendo eles o conjunto *Validators* e o conjunto *Observer* (SHCHERBAKOV, 2019).

O conjunto *Validator* é quem gerencia a escrita, são os nodos que de fato participam do protocolo de consenso. Já o conjunto *Observer* serve para gerenciar a leitura. Dessa forma, se é feita uma requisição de leitura ela é direcionada ao *Observer Pool*, se no caso for uma requisição de escrita ela é enviada para o *Validator Pool*. Os *Observer* servem para aliviar a carga dos *Validators*, realizando as leituras e deixando o processamento do consenso e escrita para o *Validator*.

É no *Validator Pool* que o consenso está implementado, o Indy-Plenum utiliza o algoritmo *Redundant Byzantine Fault Tolerance* (CURRAN; PASTUCHOV, 2019). A comunicação nodo-a-nodo é baseado em TCP utilizando *Authenticated Encryption*, sem assinaturas digitais. Já as requisições para a comunicação nodo-cliente - considerando que as requisições de escrita

vão para os nodos *Validator* - necessitam de uma assinatura.

Ainda no *Validator Pool*, no protocolo de consenso, na hora da escrita todos os nodos assinam em conjunto. Essa assinatura é utilizada para verificação de dados.

Como o Registro Distribuído Indy requer permissão para escrita, toda requisição de escrita deve ser assinada. A requisição é enviada para todos os nodos do *Validator Pool* e espera-se $F + 1$ respostas para ter certeza que a requisição foi escrita. Segue na Figura 11 um exemplo de transação de escrita.

As requisições de leitura não necessitam assinaturas, como o Registro é de acesso público, qualquer um pode ler. As requisições de leitura são enviados para o *Observer Pool*, porém é enviado para apenas um nodo e espera-se apenas uma resposta. É possível confiar na resposta por causa das assinaturas agregadas na hora da escrita – a resposta vem com provas de que pertence àquela árvore Merkle, e que aquela árvore Merkle pertence àquele conjunto de nodos – As escritas no Registro são assinadas por todos os nodos.

Figura 11 – Exemplo de escrita de esquema no Indy.

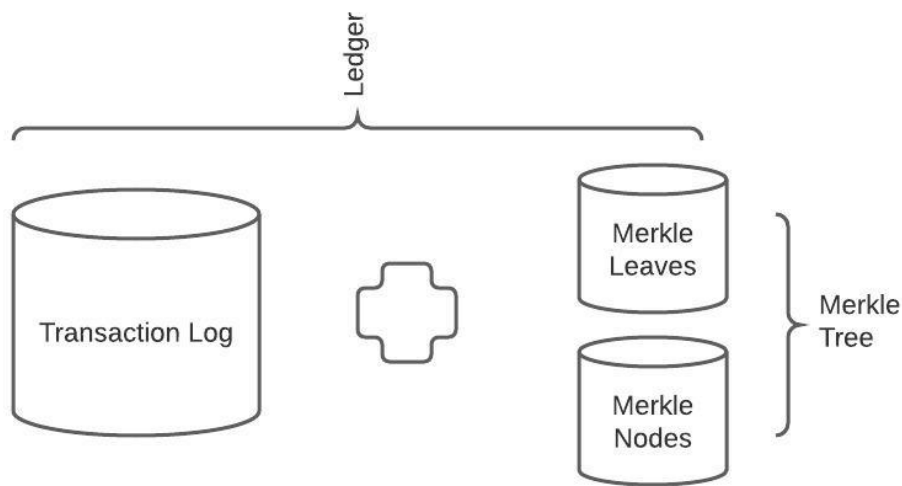


Fonte – Inspirado em Indyscan (2021)

4.3 REGISTRO DISTRIBUÍDO

O Blockchain/Registro Distribuído é uma base de dados replicada em todo nodo. O Registro Distribuído da implementação do Hyperledger Indy, consiste em um log ordenado das transações e uma árvore Merkle (HYPERLEDGER, 2018a), como consta na Figura 12. Árvore Merkle é uma estrutura de dados recorrente em implementações de Blockchain pois como visto acima é uma forma simples de checar a consistências dos dados, verificando se todos os valores da Raiz da árvore de Merkle são os mesmos em todos os nodos.

Figura 12 – Composição do Registro Distribuído Hyperledger Indy.



Fonte – Inspirado em Shcherbakov (2019).

4.4 TIPOS DE REGISTROS DISTRIBUÍDOS

O Hyperledger Indy opera com quatro Registros diferentes, todos eles seguem a mesma lógica da Figura 12: uma lista de transações e uma árvore Merkle. Esses Registros são o Config Ledger, Pool Ledger, Domain Ledger e Audit Ledger (HYPERLEDGER, 2018b).

4.4.1 Config Ledger

Primeiro temos o Config Ledger, onde ficam registrados informações a respeito das validações de transações, políticas de autorização e etc (HYPERLEDGER, 2018a). São informações/configurações que todos os nodos devem saber em consenso. Os nodos leem esse Registro para estar a par dessas configurações.

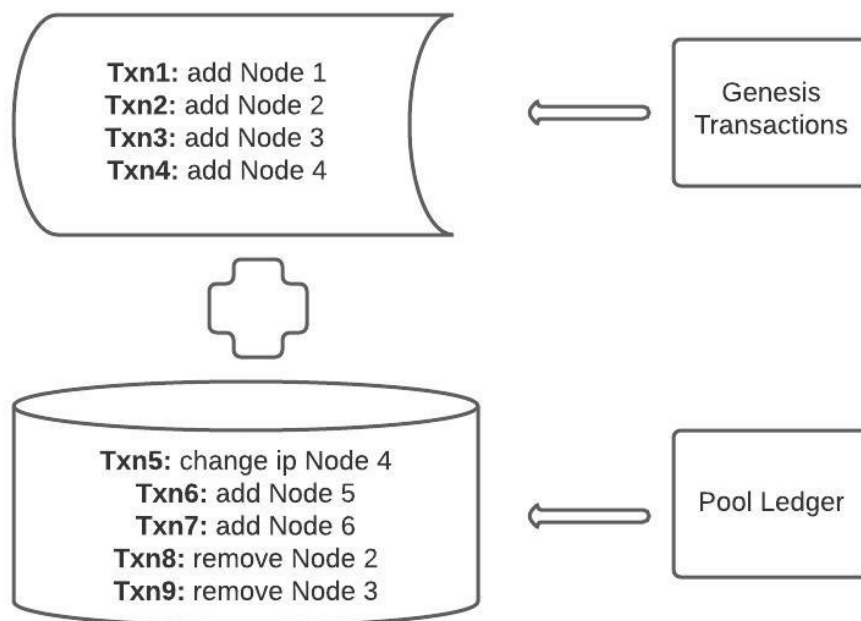
4.4.2 Pool Ledger

No Pool Ledger ficam registradas informações sobre o estado atual do Conjunto de Nodos (HYPERLEDGER, 2018a) – quem são os nodos, suas chaves públicas, ips e etc – Toda transação que adiciona, remove ou edita nodos é registrada aqui. Mais uma vez, todos os nodos da rede leem desse Registro para saberem quem são os outros nodos do Conjunto de Nodos e como se comunicar com eles.

Esse Registro precisa de um “motor de arranque” que é o *Gênesis File*. Como todas as informações sobre o Conjunto de Nodos estão armazenados no próprio Pool Ledger, então, quando o Pool Ledger está em branco, iniciando do zero, ele não possui informação nenhuma sobre o Conjunto de Nodos. Não é possível saber quem faz parte do pool, quais seus ips e etc. O Gênesis File é esse “motor de arranque” que faz as primeiras transações no Pool Ledger – ao rodar pela primeira vez, ele lê o Gênesis File e escreve no Pool Ledger. O *Gênesis File* deve conter as informações iniciais do Conjunto de Nodos (quem são os nodos, quais seus ips, etc), assim quando um nodo roda pela primeira vez ele sabe onde conectar. O *Gênesis File* é lido apenas na primeira vez que o Pool Ledger é executado (HYPERLEDGER, 2018a).

Após as transações iniciais do Gênesis File, seguem no Pool Ledger todas as transações subsequentes referentes ao Conjunto de Nodos, como mostrado na Figura 13.

Figura 13 – Pool Ledger.



Fonte – Inspirado em Shcherbakov (2019).

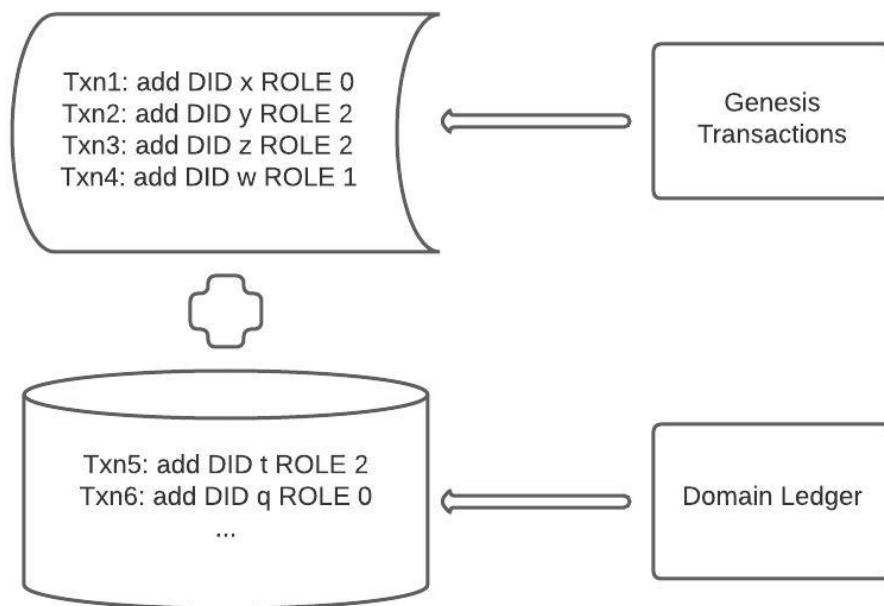
4.4.3 Domain Ledger

O Domain Ledger é o Registro principal, onde ficam as transações específicas de identidade e de aplicação (HYPERLEDGER, 2018a). De forma análoga ao Pool Ledger, o Domain Ledger também precisa de um Gênesis File.

Para escrever no Registro é necessário uma identidade com papel/permissão de escrita, porém as informações sobre todas as identidades encontram-se no próprio Domain Ledger, se o Registro está em branco, não há como criar nenhuma identidade nova pois não existe autorização para escrever no Registro. Novamente o “motor de arranque” é necessário. O Gênesis File escreve as primeiras transações no Registro, colocando algumas identidades que possuem papel que permitam a escrita – registra o usuário inicial que adicionará os outros. A Figura 14 representa o Domain Ledger.

Na sequência às transações do Gênesis File, seguem todas as transações subsequentes de identidade e de aplicação.

Figura 14 – Domain Ledger.



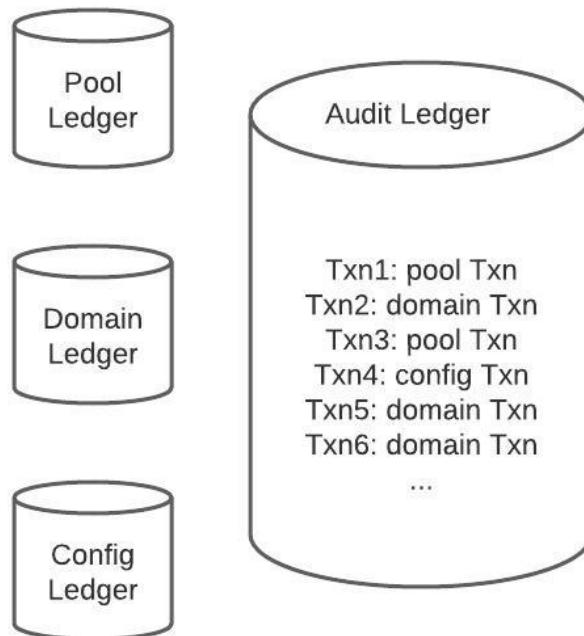
Fonte – Inspirado em Shcherbakov (2019).

4.4.4 Audit Ledger

O Audit Ledger é o Registro responsável pela sincronização entre as diferentes Ledgers. Esse Registro monitora as outras Ledgers e ordena todas as transações de todas as Ledgers em uma sequência que representa todas as transações do sistema de forma ordenada (HYPERLEDGER, 2018b).

Esse registro é utilizado para recuperação do sistema e também para auditorias externas, além de gerar controle e coesão interna para o sistema. A Figura 15 representa o Audit Ledger.

Figura 15 – Audit Ledger.



Fonte – Inspirado em Shcherbakov (2019).

5 HYPERLEDGER ARIES

Hyperledger Aries é uma biblioteca pertencente à comunidade Hyperledger. Tem como objetivo prover soluções para criar, transmitir e armazenar Credenciais Verificáveis. Aries utiliza o apoio de outra biblioteca, Hyperledger Ursa, para suporte criptográfico (HYPERLEDGER, 2020).

Aries permite interações ponto-a-ponto baseado em identidades descentralizadas, e suporta diversos registros distribuídos diferentes. Junto com Hyperledger Indy e Hyperledger Ursa, faz parte dos projetos Hyperledger voltados para implementação de sistemas de Identidade Auto-Soberana.

A biblioteca Aries possui uma camada de interface para criar, assinar e ler transações na blockchain. Fornece suporte para trocas e emissão de Credenciais Verificáveis, incluindo credenciais que utilizam as premissas de zero conhecimento, encontrados na biblioteca Ursa.

5.1 ARIES AGENT

Um Agente é uma peça de software com o propósito de interagir com outras entidades, via DIDs e também por outros meios. Uma instância de um Agente Aries é composta por duas partes, o agente e o controlador, como mostrado na Figura 16. O Aries Agent é o responsável por gerir as funcionalidades principais do Aries (HYPERLEDGER, 2021), incluindo interação com outros agentes, gerenciamento de armazenamento seguro, além de troca de mensagem com o controlador.

O controlador é quem provê a lógica de negócio, indicando como o agente deve responder a eventos. O Agente envia notificações de evento para o controlador, que por sua vez analisa a melhor resposta e envia mensagens administrativas para o Agente (HYPERLEDGER, 2021). A comunicação entre os dois é feita por meio de webhooks e chamadas HTTP.

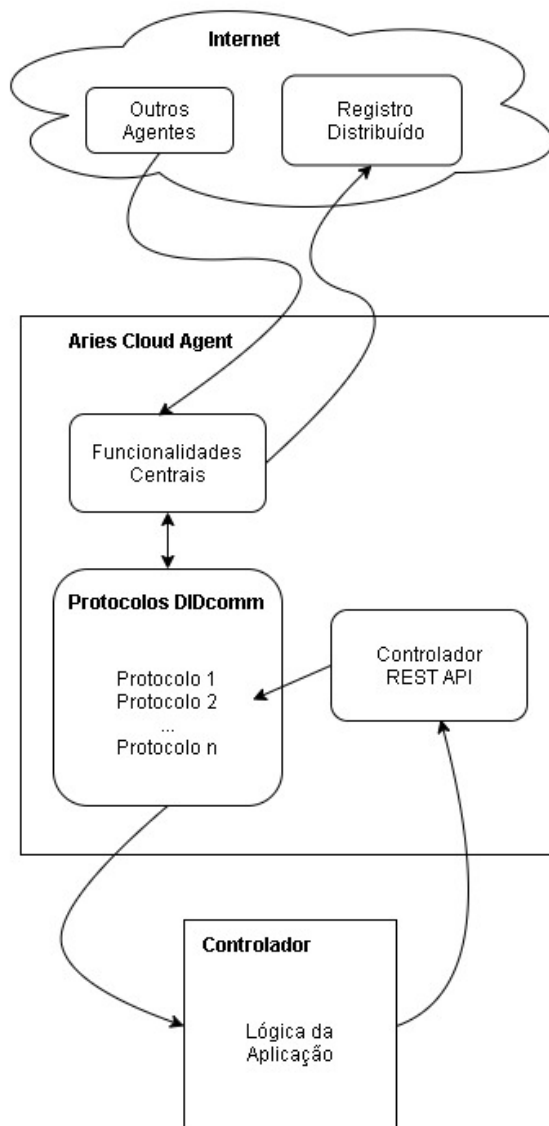
Assim, para desenvolver projetos com o Aries, na maioria dos casos basta programar o controlador, que proverá a lógica de negócios.

Na arquitetura de uma rede utilizando Hyperledger Indy e Hyperledger Aries, existem diversos agentes. Os agentes que se encontram nas "bordas" desta rede, são aqueles contidos em celulares, tablets, computadores, etc. Temos também os agentes na "nuvem" que oferecem roteamento de mensagens. Assim, geralmente, enquanto os agentes da "borda" são pessoas e organizações, os agentes da nuvem tem principalmente como lógica de negócio o roteamento de mensagens entre agentes. Mensagens enviadas entre dois agentes da borda são roteados por agentes na nuvem (HYPERLEDGER, 2021).

5.2 DIDCOMM

A comunicação entre agentes acontece por meio de um mecanismo de mensagem chamado DIDcomm (DID Communication). DIDcomm permite uma troca segura e assíncrona de

Figura 16 – Estrutura interna de um Agente Aries.



Fonte – Inspirado em Hyperledger (2021)

mensagens encriptadas ponto-a-ponto, que geralmente são roteadas por meio de agentes Aries intermediários. A criptografia é feita pela biblioteca Hyperledger Ursa.

O mecanismo usa uma instância do método `did:peer DID method`, que faz uso de DIDs não publicados na blockchain, utilizados apenas de forma privada entre os dois agentes que se comunicam (HYPERLEDGER, 2021). Entre os protocolos padrões definidos, que configuram um conjunto de mensagens para realizar determinada tarefa, podemos destacar:

- O protocolo “estabelecer conexão” (establish connection) que permite a conexão de dois agentes por meio de um conjunto de mensagens: o convite, a requisição de conexão e a resposta de conexão.
- O protocolo “emitir credencial” (issue credential) que permite um agente emitir uma credencial para outro agente.

- O protocolo “apresentar prova” (present proof) que permite que agentes façam requisições e recebam provas de outros agentes.

6 PASSAPORTE COVID

Nesse contexto do recente surto de Covid-19, o paradigma de Identidade Auto-Soberana é útil. Com as tecnologias e ferramentas discutidas acima, é possível criar uma gestão de identidade que respeita a privacidade e a propriedade dos dados, por meio de mecanismos de divulgação seletiva e provas de zero conhecimento.

O período pós pandemia também gerará desafios próprios. Países tentam reabrir suas economias da forma mais segura possível, e alguns países, cidades e estados começam a requerer comprovantes de imunização, os chamados “passaporte Covid”, como o caso da cidade de São Paulo que passou a exigir tal passaporte para eventos com mais de 500 pessoas (PREFEITURA de São Paulo, 2021).

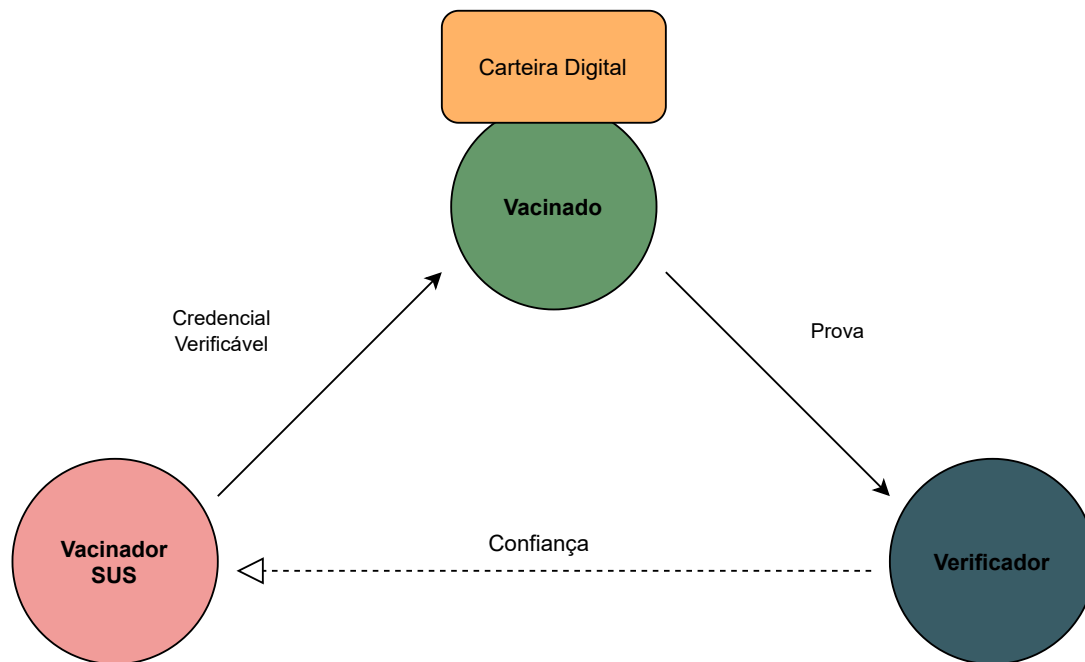
Dessa forma, percebendo tal relevância, propomos a implementação de um caso de uso de um “passaporte Covid”. Uma credencial verificável, que pode ser emitida pelos órgãos de saúde e permite que o cidadão possua sua prova de vacinação no celular. Tal credencial contém dados de identificação do cidadão tais como nome, endereço, nascimento, e também dados a respeito da vacinação, como dose (primeira, segunda ou terceira), laboratório provedor da vacina e órgão vacinador.

O ecossistema se configura tal a Figura 17 mostra: Um emissor, no nosso caso, alguma entidade relacionada ao SUS, emite uma credencial verificável para o paciente vacinado. Esse paciente armazena tal credencial em uma carteira digital, e por meio dessa carteira ele é capaz de apresentar as provas de sua vacinação para as partes interessadas, no caso proposto, locais públicos, tais como aeroportos, farmácias, cinemas, casa de shows, etc. O verificador confia nas provas pois ele confia no emissor. A chave de verificação e o DID do emissor está registrado na blockchain, onde o verificador pode verificar que aquela credencial é proveniente daquele emissor.

Para apresentar a prova de vacinação, serão utilizado técnicas de divulgação seletiva e zero conhecimento, de forma que a exposição dos dados seja a mínima possível. Para a comprovação da vacinação é apenas necessário afirmar se o número de doses é maior ou igual àquele requerido por quem verifica a vacinação. É possível também revelar dados chave necessário em situações específicas, como o nome do laboratório, ou a idade do paciente.

Essa técnica de divulgação é possível graças ao esquema de assinatura Camenisch-Lysyanskaya aplicado às credenciais, onde cada campo de um credencial verificável é assinado, assim é possível divulgá-los de forma isolada (YOUNG, 2020). Essa assinatura também permite provas de predicado.

Figura 17 – Papeis envolvidos no sistema proposto .



Fonte – Inspirado em Reed, Joosten e Deventer (2021)

7 IMPLEMENTAÇÃO

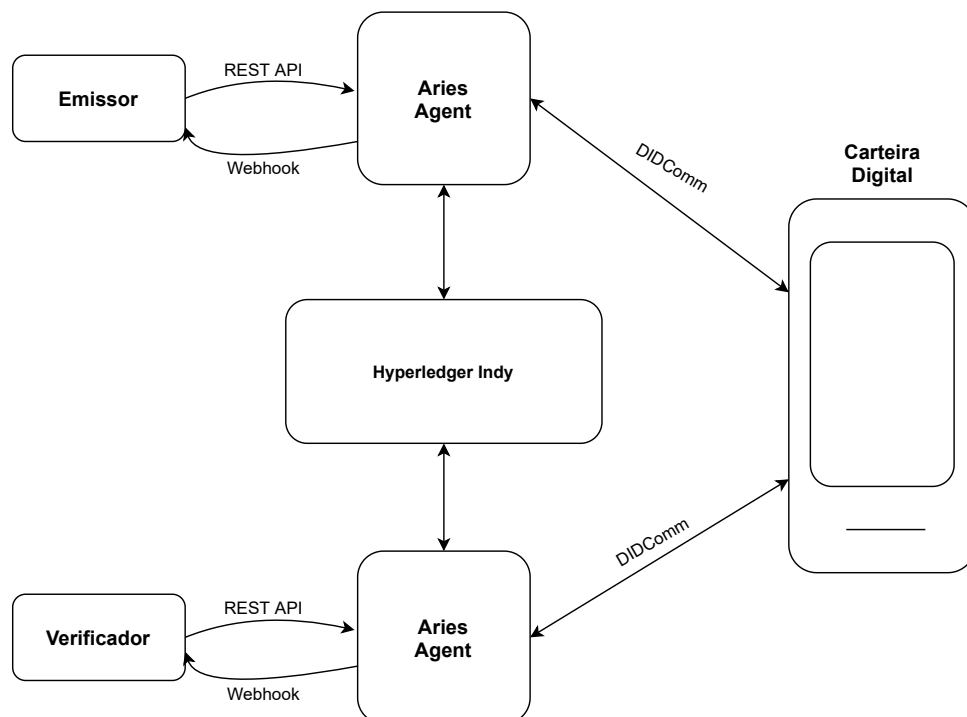
7.1 FERRAMENTAS UTILIZADAS

Na parte de estudo das ferramentas existentes, ficou claro que o Hyperledger Indy é o ecossistema de código livre mais maduro voltado para implementações de Identidade Auto-Soberana, portanto é um candidato excelente para ser usado como o registro distribuído em nosso protótipo. Os esquemas de credenciais, definições de credenciais, DIDs públicos e chaves públicas ficam gravados no registro distribuído Indy.

O Hyperledger Aries é advindo do projeto Hyperledger Indy, porém se separou em um projeto próprio. Hyperledger Aries é responsável pela criação e emissão de credenciais verificáveis. O Aries opera como uma interface entre os emissores/verificadores, o registro Indy e as carteiras digitais. Tanto o Hyperledger Indy como o Hyperledger Aries utilizam a biblioteca criptográfica Hyperledger Ursa.

Para que os emissores e verificadores se comuniquem com o Hyperledger Aries, foi criado um serviço web que faz chamadas API para os agentes Aries. O modelo final do protótipo é mostrado tal qual a Figura 18.

Figura 18 – Arquitetura do protótipo proposto.



Fonte – O autor.

A rede Sovrin é regida pela Fundação Sovrin, uma fundação independente que é responsável por assegurar que o sistema de identidade Sovrin seja público e acessível globalmente (SOVRIN, 2021). A rede Sovrin é pública e permissionada. É a implementação do Hyperledger Indy mais madura em produção. Possui três redes: A rede principal de produção MainNet, a

rede de pré-produção StagingNet para protipação e a rede de testes BuilderNet. Por ser a principal implementação do Hyperledger Indy, optamos por utilizar a StaginNet da rede Sovrin como nosso registro distribuído, uma opção simples de utilizar. A comunicação com a rede Sovrin é feita por meio de *endpoints*.

O software Verity, produzido pela empresa Evernym (EVERNYM, 2021), é um serviço de agente na nuvem, do tipo software-as-a-service (SaaS). Verity implementa os protocolos de comunicação do Hyperledger Aries. O software Verity é uma maneira simples de implementar um agente Aries, pois funciona como um servidor onde enviamos chamadas REST e ele retorna Webhooks. Esse servidor permite ao desenvolvedor se comunicar por DIDComm com as carteiras digitais e também com o registro distribuído. Por essas facilidades, optamos por utilizar o servidor Verity como nosso agente Aries.

Por fim, A carteira digital para mobile Connect.me (EVERNYM, 2018), também produzida pela empresa Evernym, oferece compatibilidade com as ferramentas acima citadas, uma solução gratuita que permite conexões únicas baseadas em DIDs. No contexto do protótipo, as credenciais verificáveis emitidas devem ser armazenadas em carteiras digitais.

7.2 PROTÓTIPO

Munido das ferramentas acima citadas, com a rede Sovrin operando como o registro distribuído Hyperledger Indy, o servidor da Verity tratando das comunicações DIDComm oferecidas pelo Hyperledger Aries, e finalmente a carteira Connect.me para armazenamento das credenciais, configura todas as partes para que o protótipo de uma credencial verificável Passaporte Covid possa ser implementada.

A última etapa desse ecossistema foi a criação de serviços web representando tanto o emissor como o verificador, para realizar as chamadas REST e comunicar-se com o restante do sistema. O emissor e o verificador foram realizados por meio de HTML e Javascript. Com esses sistema é possível montar uma credencial verificável para provar a vacinação, como descrito a seguir.

A operação do protótipo segue o seguinte fluxo:

- Emissor registra DID no Indy.
- Emissor registra Esquema de Credencial no Indy.
- Emissor registra Definição de Credencial no Indy.
- Emissor conecta-se com a carteira digital do paciente.
- Emissor emite credencial que fica armazenada na carteira digital.
- Verificador conecta-se a carteira digital do paciente.
- Verificador envia requisição de prova para a carteira do paciente.

- Paciente compartilha a prova de vacinação.

Na Figura 19a vemos a tela inicial de tal sistema. o primeiro passo a ser feito é registrar um DID para o emissor no registro distribuído Indy da Sovrin, no protótipo tal DID pertence a alguma entidade vinculada ao SUS. Esse registro é realizado por meio de chamadas API, assim ao clicar no botão "Cadastrar Emissor", como visto na Figura 19b, é gerado um par de chaves para DID e enviado por meio de chamadas REST para a interface do Hyperledger Aries, que por sua vez o envia para a rede Sovrin onde é registrado de forma permanente no registro distribuído. Por meio do site Indy Scan (INDYSCAN, 2021) podemos acompanhar todas as transações realizadas na rede Sovrin, assim, na Figura 24 do apêndice A podemos visualizar a transação realizada para o registro do DID do emissor.

Tendo sido o emissor devidamente registrado na rede Sovrin, ele torna-se capaz de fazer novas transações na rede, como emitir um modelo de esquema de credencial que será utilizado. O esquema de credencial do protótipo conta com os seguintes campos: nome, endereço, nascimento, laboratório, dose e vacinador, como mostrado na Figura 19c, a tela do protótipo, e pela Figura 25 do apêndice A, a transação na rede Sovrin de tal esquema.

Após a emissão do esquema, seguindo o fluxo, é necessário registrar também no registro distribuído a definição de credencial. Nessa etapa, é associada essa definição de credencial ao DID do emissor, em nosso caso o vacinador, vinculado ao SUS. A Figura 19d mostra a tela do protótipo ao emitir a definição de credencial chamada "Credencial Passaporte Imunidade", enquanto a Figura 26 do apêndice A mostra essa transação realizada na rede Sovrin.

Tendo o emissor sendo registrado na rede Sovrin, emitido seu esquema de credencial e também sua definição de credencial, está ele devidamente preparado para emitir de fato a credencial verificável com o comprovante de vacinação. Primeiramente o emissor inicia um relacionamento com a carteira digital do paciente vacinado. O sistema do emissor gera um QR Code com o convite para o relacionamento, que é lido pelo celular do paciente, como mostrado nas Figuras 20a e 20b.

Após o paciente ler e aceitar a conexão, um DID é gerado que representa o relacionamento entre o emissor e o paciente. Estando os dois conectados, o emissor pode emitir para o paciente a credencial.

A Figura 21a representa a emissão dessa credencial. O nome da credencial no exemplo é "Vacinação Maurício Barros", devidamente preenchida com os campos nome, nascimento, endereço, laboratório, dose e vacinador. Essa primeira credencial contém o valor da primeira dose preenchida.

De forma a receber a credencial, o paciente deve aceitar a credencial em seu celular, como mostrado na Figura 21b. Agora o paciente possui sua credencial verificável que demonstra a vacinação de sua primeira dose. Já é possível oferecer tais provas para um possível verificador.

Em nosso exemplo, a tela inicial do verificador é tal como representada na Figura 22a. De forma análoga ao emissor, o primeiro passo é conectar-se com a carteira digital do paciente,

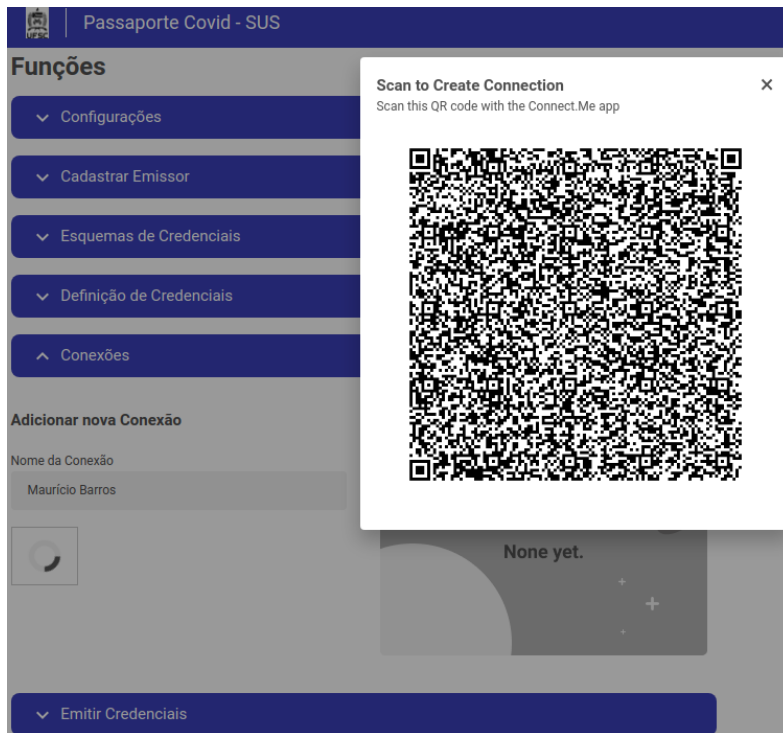


Figura 19 – Telas do protótipo

operação realizada da mesma forma que com o emissor, primeiro é gerado um convite com o QR Code e o paciente deve escanear esse convite a aceitar a conexão, como mostrado na Figura 22b.

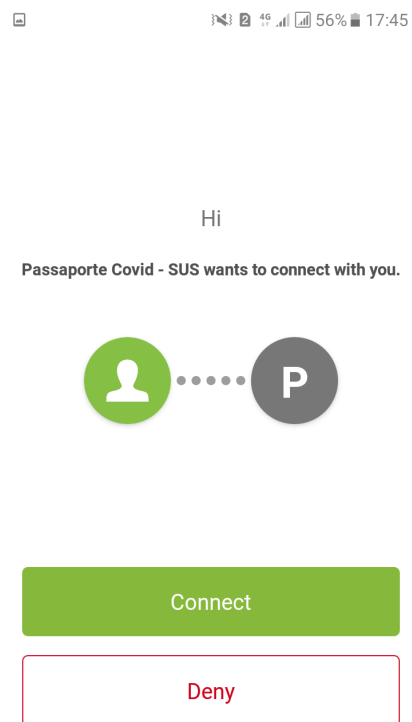
Com o verificador conectado ao paciente, já é possível para o verificador fazer a requisição da prova de vacinação. Como representado pela Figura 23a, o nome da requisição é "Vacinado 1º dose". O verificador pede a divulgação do campo "laboratório" e também, por

(a) O sistema gera um QR Code com o convite.



Fonte O autor.

(b) Após ler o QR Code, o paciente aceita a conexão.



Fonte O autor.

Figura 20 – Conexão entre vacinador e vacinado.

meio de predicados de prova, pede uma verificação se o valor do campo "dose" contida na credencial do paciente é maior ou igual ao valor 1.

Tal requisição de prova chegará como uma notificação no celular do portador da credencial, que deve aceitar a requisição para que ela possa ser enviada para o verificador, como mostra a Figura 23b.

Após o portador da credencial aceitar compartilhar os atributos requisitados, as provas serão enviadas ao verificador como pode ser visto na Figura 23c. Caso o valor do campo "dose" seja menor que 1, o portador não é capaz de enviar tal prova.

Como contraexemplo, foi requisitado uma prova de verificação da terceira dose da vacina, ou seja, uma requisição de prova onde o valor do campo "dose" deverá ser maior ou igual a três. Como o portador da credencial não possui tal valor, não é possível compartilhar tal prova, como é mostrado na Figura 23d, onde a única opção do portador é rejeitar a requisição de prova, tendo em vista que é incapaz de provar o valor da terceira dose.

7.3 RESULTADOS

Com esse arranjo foi possível concluir o protótipo de uma credencial verificável para um comprovante de vacinação "Passaporte Covid". O emissor se cadastrou na rede Sovrin, emitiu um esquema de credencial e uma definição de credencial, por fim emitiu a credencial

(a) Tela emissão de credencial verificável.

Funções

Nome da Credencial
Vacinação Maurício Barros

DID do relacionamento
T77eDYWaxLygMG43aAiWET

Id da Definição de Credencial
GTrQG45mrDAkRZw8Fbdguh:3:CL:259582:latest

Valores da Credencial (em JSON)
["Nome": "Maurício Barros", "Nascimento": "09/01/1987", "Endereço": "Rua Teste, 21", "Laboratório": "Butantan", "Dose": 1, "Va"]

Emitir Credencial

Fonte O autor.

(b) O paciente deve aceitar a credencial emitida.

Credential Offer

Passaporte de Imunidade

Dose
1

Endereço
Rua Teste, 21

Laboratório
Butantan

Nascimento
09/01/1987

Nome
Maurício Barros

Vacinador
Posto 1

Accept Credential

Reject

Fonte O autor.

Figura 21 – Emissão do comprovante de vacinação.

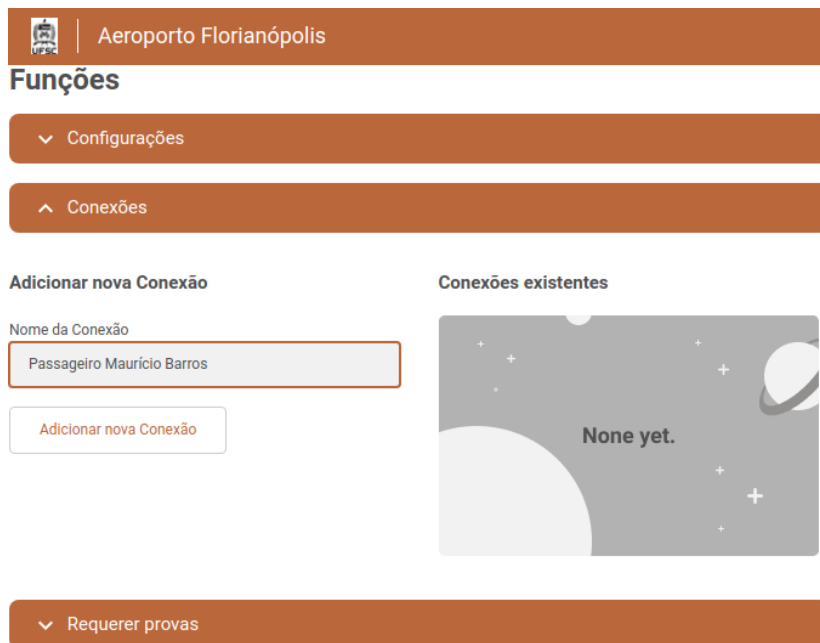
verificável contendo o comprovante de vacinação.

O portador da credencial por sua vez, aceitou a credencial que ficou armazenada em uma carteira digital em seu celular, podendo apresentá-la quando necessário.

Todo o arranjo permite divulgação seletiva e provas de zero conhecimento. Foi possível comprovar a vacinação do portador da credencial, mostrando apenas o nome do laboratório e se o número de doses é maior ou igual àquele requerido pelo verificador. Tal arranjo garante privacidade de todos os outros dados do portador que não são necessários para provar a vacinação.

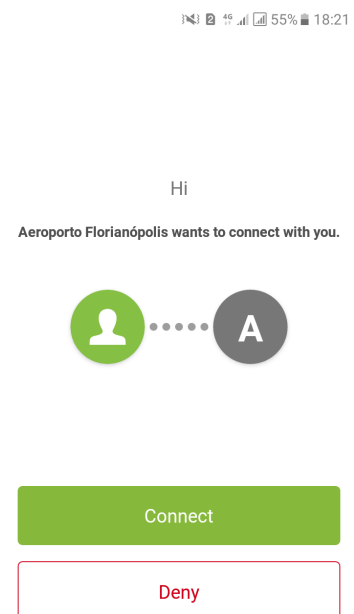
Em um cenário onde o comprovante de vacinação seja em formato de papel, todos os dados do portador seriam expostos, tornando uma verificação mais invasiva.

(a) Tela inicial do verificador.



Fonte O autor.

(b) O paciente deve aceitar a conexão com o verificador.



Fonte O autor.

Figura 22 – O verificador se conecta ao portador da credencial.

(a) Requisição de prova primeira dose.

Funções

Configurações

Conexões

Requerer provas

Enviar requisição de prova

Nome da requisição de prova
Vacinado 1° dose

DID do relacionamento
HzRejq87UMfz1WbChdxF2

JSON do conjunto de provas de atributos
[{"name": "Laboratório"}]

JSON do conjunto de predicados de provas
[{"name": "dose", "p_type": ">=", "p_value": 1}]

Enviar requisição de provas

Provas recebidas

None yet.

Fonte O autor.

(b) O portador da credencial deve aceitar a requisição de prova.

Proof Request

Requested by

Aeroporto Florianópolis

A

Vacinado 1° dose

Laboratório

Butantan

P

dose

Greater than or equal to 1

P

Share Attributes

Reject

Fonte O autor.

(c) Provas recebidas pelo verificador.

Funções

Configurações

Conexões

Requerer provas

Enviar requisição de prova

Nome da requisição de prova

DID do relacionamento
-- selecionar uma opção --

JSON do conjunto de provas de atributos
[{"name": "first_attr"}, {"name": "second_attr"}]

JSON do conjunto de predicados de provas

Enviar requisição de provas

Provas recebidas

DID do relacionamento
HzRejq87UMfz1WbChdxF2
Data
{"revealed_attrs": {"Laboratório": {"identifier_index": 0, "value": "Butantan"}}, "self_attested_attrs": {}, "unrevealed_attrs": {}, "predicates": {"dose": {"identifier_index": 0}, "identifiers": [{"schema_id": "GTrQG45mrDAkRZw8Fbdguh:2:Passaporte de Imunidade:1.0", "cred_def_id": "GTrQG45mrDAkRZw8Fbdguh:3:CL:259582:latest"}]}}

Fonte O autor.

(d) O portador não consegue provar que possui a terceira dose.

Proof Request

Requested by

Aeroporto Florianópolis

A

Passageiro Vacinado 3° dose

Laboratório

Butantan

P

Dose

Greater than or equal to 3

!

Share Attributes

Reject

Fonte O autor.

Figura 23 – Requisição de provas

8 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

8.1 CONSIDERAÇÕES FINAIS

O desenvolvimento do presente estudo possibilitou um levantamento de temas, ferramentas e tecnologias que permitem o uso do modelo de Identidade Auto-Soberana. Utilizando a ferramenta Hyperledger Indy para o registro distribuído possibilita a diminuição da centralização. A rede Indy fornece a capacidade de oferecer confiança. O emissor (das credenciais) tem seu DID e sua chave de verificação registrados na Blockchain, que são checados pelo verificador. Enquanto a rede distribuída estiver funcionando, o registro continuará disponível.

Os protocolos do Hyperledger Aries fornecem interface entre diferentes atores, emissão e gerenciamento de credenciais verificáveis, se comunica com a carteira digital e com o registro distribuído. Suas interações sempre amparadas pelas bibliotecas criptográficas do Hyperledger Ursa.

Essa tríade de projetos, Indy, Aries e Ursa oferecem em conjunto um ecossistema onde diversas implementações de modelos de Identidade Auto-Soberana podem existir. Esses novos modelos trazem maior privacidade, segurança e propriedade para os dados de usuários.

Com sucesso, utilizando esse modelo, o presente trabalho foi capaz de montar um sistema de emissão e verificação de credenciais, amparado pela tecnologia Blockchain e funções criptográficas. Tal protótipo gerou um certificado de vacinação que garante mecanismos de divulgação seletiva e provas de zero conhecimento. Este certificado, que é custodiado pelo próprio vacinado, garante a comprovação da vacinação com grande nível de privacidade de seus dados, diferindo-se de outros modelos de identidade.

Apesar de possíveis polêmicas a favor ou contra os ditos “passaportes de vacinação”, credenciais verificáveis, com divulgação seletiva, tornam o seu uso menos invasivo. Dessa forma, aliviando o peso das inúmeras mudanças que o mundo inteiro vem realizando para se adaptar à pandemia e seus efeitos.

A medida que cada vez mais pessoas vão percebendo a importância de um tratamento adequado de seus dados digitais, o tema de privacidade ganhará mais importância. Provavelmente ainda teremos um longo caminho para aperfeiçoar o trato de nossos dados. Esse caminho perpassará modelos de gestão de identidades tais como o de Identidade Auto-Soberana.

No futuro que se aproxima, novas políticas, mecanismos e paradigmas de gerenciamento de dados serão criados, provavelmente novas legislações, conforme passamos mais tempo de nossas vidas no mundo online. Paradigmas como a Identidade Auto-Soberana farão parte desse futuro, suas tecnologias como Blockchain e suas ferramentas como Hyperledger Indy e Aries, provavelmente crescerão e ficarão mais robustas conforme vamos nos adaptando a novas realidades digitais. O futuro é digital, e nossos dados são e devem ser nossos.

8.2 TRABALHOS FUTUROS

Podemos citar como possíveis trabalhos futuros:

- Aperfeiçoamento do protótipo, adicionando algum tipo de revogação e tornando a interface gráfica o mais simples possível. Gerar *Templates* de requisição de prova pré-feitos.
- Realização de testes de rede, verificar as capacidades de emissão do sistema.
- Expandir o modelo de credencial para ser utilizado de forma genérica em outros casos de uso.

REFERÊNCIAS

- ALLEN, C. **The path to self-sovereign identity**. 2016. Disponível em: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>. Acesso em: 04 abr. de 2021.
- BOKKEM, D. van et al. **Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology**. 2019.
- BRASIL. Lei geral de proteção de dados pessoais (lgpd). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 set. de 2021.
- CURRAN, S.; PASTUCHOV, A. **Introduction to Hyperledger Indy**. 2019. Disponível em: <https://github.com/hyperledger-archives/education/blob/master/LFS171x/docs/introduction-to-hyperledger-indy.md>. Acesso em: 16 ago. de 2021.
- EVERNYM. **Connect.me**. 2018. Disponível em: <https://www.connect.me/>. Acesso em: 10 mai. de 2021.
- EVERNYM. **Building SSI solutions has never been easier**. 2021. Disponível em: <https://www.evernym.com/products/#credentials>. Acesso em: 22 mai. de 2021.
- FAPESP. **FAPESP COVID-19 DataSharing/BR**. 2020. Disponível em: <https://repositoriodatasharingfapesp.uspdigital.usp.br/>. Acesso em: 8 set. de 2021.
- FERDOUS, M. S.; CHOWDHURY, F.; ALASSAFI, M. O. In search of self-sovereign identity leveraging blockchain technology. **IEEE Access**, v. 7, p. 103059–103079, 2019.
- HARIKRISHNAN, M.; LAKSHMY, K. Secure digital service payments using zero knowledge proof in distributed network. In: **2019 5th International Conference on Advanced Computing Communication Systems (ICACCS)**. [S.l.: s.n.], 2019. p. 307–312.
- HYPERLEDGER. **Hyperledger Indy**. 2015. Disponível em: <https://www.hyperledger.org/use/hyperledger-indy>. Acesso em: 03 mai. de 2021.
- HYPERLEDGER. **Welcome to Hyperledger Indy Node's documentation**. 2018. Disponível em: <https://hyperledger-indy.readthedocs.io/projects/node/en/latest/index.html>. Acesso em: 03 mai. de 2021.
- HYPERLEDGER. **Welcome to Indy Plenum's documentation**. 2018. Disponível em: <https://hyperledger-indy.readthedocs.io/projects/plenum/en/latest/index.html>. Acesso em: 03 mai. de 2021.
- HYPERLEDGER. **Hyperledger Aries**. 2020. Disponível em: <https://github.com/hyperledger/aries>. Acesso em: 16 ago. de 2021.
- HYPERLEDGER. **Becoming a Indy/Aries Developer**. 2021. Disponível em: <https://github.com/hyperledger/aries-cloudagent-python/tree/main/docs/GettingStartedAriesDev>. Acesso em: 11 jun. de 2021.

IBRAHEM, M. K. Modification of diffie-hellman key exchange algorithm for zero knowledge proof. In: **2012 International Conference on Future Communication Networks**. [S.l.: s.n.], 2012. p. 147–152.

INDYSCAN. **Indyscan Hyperledger Indy transaction explorer**. 2021. Disponível em: https://indyscan.io/home/SOVRIN_STAGINGNET. Acesso em: 10 set. de 2021.

ISO. **ISO/IEC 24760-1:2019(en) IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts**. 2019. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en>. Acesso em: 12 jun. de 2021.

ITI. **icp - brasil**. Instituto Nacional de Tecnologia da Informação, 2021. Disponível em: <https://estrutura.iti.gov.br/>. Acesso em: 10 set. de 2021.

KIM, B. G. et al. A security analysis of blockchain-based did services. **IEEE Access**, v. 9, p. 22894–22913, 2021.

LIM, S. Y. et al. Blockchain technology the identity management and authentication service disruptor: A survey. **International Journal on Advanced Science, Engineering and Information Technology**, v. 8, p. 1735, 09 2018.

LINUX FOUNDATION. **Hyperledger**. 2015. Disponível em: <https://www.hyperledger.org/>. Acesso em: 03 mai. de 2021.

MALIKI, T. E.; SEIGNEUR, J.-M. A survey of user-centric identity management technologies. In: **The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)**. [S.l.: s.n.], 2007. p. 12–17.

MÜHLE, A. et al. A survey on essential components of a self-sovereign identity. **CoRR**, abs/1807.06346, 2018. Disponível em: <http://arxiv.org/abs/1807.06346>. Acesso em: 27 set. de 2021.

NAIK, N.; JENKINS, P. Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems. In: **2020 IEEE International Symposium on Systems Engineering (ISSE)**. [S.l.: s.n.], 2020. p. 1–6.

NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 04 abr. de 2021.

NCATS. **National COVID Cohort Collaborative (N3C)**. 2021. Disponível em: <https://ncats.nih.gov/n3c>. Acesso em: 8 set. de 2021.

PREFEITURA de São Paulo. **Passaporte da Vacina será solicitado para acesso a eventos a partir desta quarta-feira em São Paulo**. 2021. Disponível em: <https://www.capital.sp.gov.br/noticia/passaporte-da-vacina-sera-solicitado-para-acesso-a-eventos-a-partir-desta-quarta-feira-em-sao-paulo>. Acesso em: 8 set. de 2021.

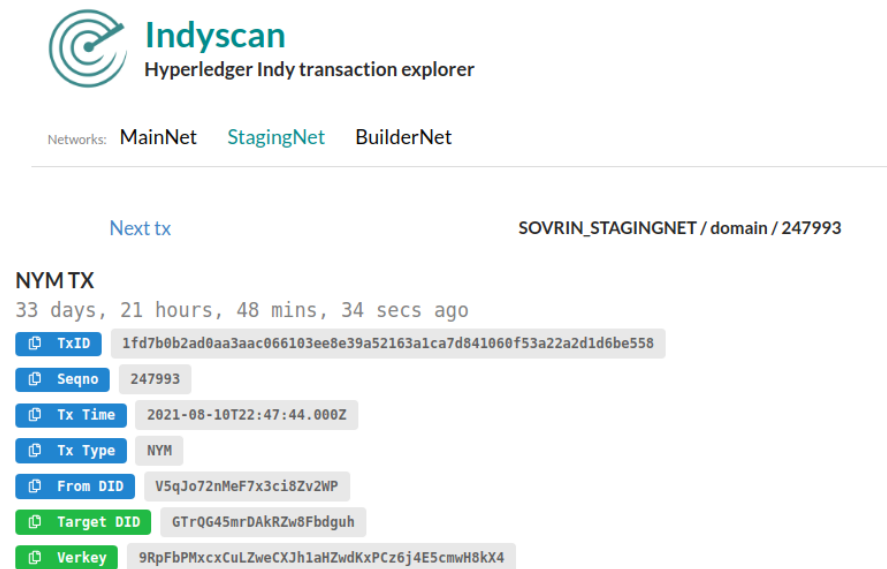
QI, M.; CHEN, B. Construction of safe patent trading platform based on zero-knowledge proof. In: **2009 Asia-Pacific Conference on Information Processing**. [S.l.: s.n.], 2009. v. 2, p. 627–630.

REED, D.; JOOSTEN, R.; DEVENTER, O. v. Self-sovereign identity: Decentralized digital identity and verifiable credentials. In: _____. Shelter Island, USA: Manning, 2021. v. 1, cap. The basic building blocks of SSI, p. 21–38. ISBN 9781617296598.

- ROSENBERG, M.; CONFESSORE, N.; CADWALLADR, C. **How Trump Consultants Exploited the Facebook Data of Millions**. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em: 3 set. de 2021.
- SCHARDONG, F.; CUSTÓDIO, R. **Self-Sovereign Identity: A Systematic Map and Review**. 2021. Disponível em: <https://arxiv.org/abs/2108.08338>. Acesso em: 20 set. de 2021.
- SHCHERBAKOV, A. **Hyperledger Indy Public Blockchain Node with Alexander Shcherbakov**. 2019. Disponível em: <https://www.youtube.com/watch?v=UJbJRqur4ng>. Acesso em: 15 mai. de 2021.
- SOVRIN. **Sovrin**. 2021. Disponível em: <https://sovrin.org/>. Acesso em: 22 mai. de 2021.
- SPORNY, M.; LONGLEY, D.; CHADWICK, D. **Verifiable Credentials Data Model 1.0**. 2019. Disponível em: <https://www.w3.org/TR/vc-data-model/>. Acesso em: 26 ago. de 2021.
- SPORNY, M. et al. **Decentralized Identifiers (DIDs) v1.0**. 2021. Disponível em: <https://www.w3.org/TR/did-core/>. Acesso em: 26 ago. de 2021.
- STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6.. ed. [S.l.]: Pearson Education do Brasil, 2015.
- YAGA, D. et al. **NISTIR 8202 Blockchain Technology Overview**. 2018. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf>. Acesso em: 26 ago. de 2021.
- YONG, J. et al. Constructing robust digital identity infrastructure for future networked society. In: **Proceedings of the 2011 15th International Conference on Computer Supported Cooperative Work in Design (CSCWD)**. [S.l.: s.n.], 2011. p. 570–576.
- YOUNG, K. **Verifiable Credentials Flavors Explained**. 2020. Disponível em: <https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf>. Acesso em: 25 set. de 2021.

APÊNDICE A – VISUALIZAÇÃO DAS TRANSAÇÕES

Figura 24 – Transação de emissão do DID do emissor vista no Indy Scan.

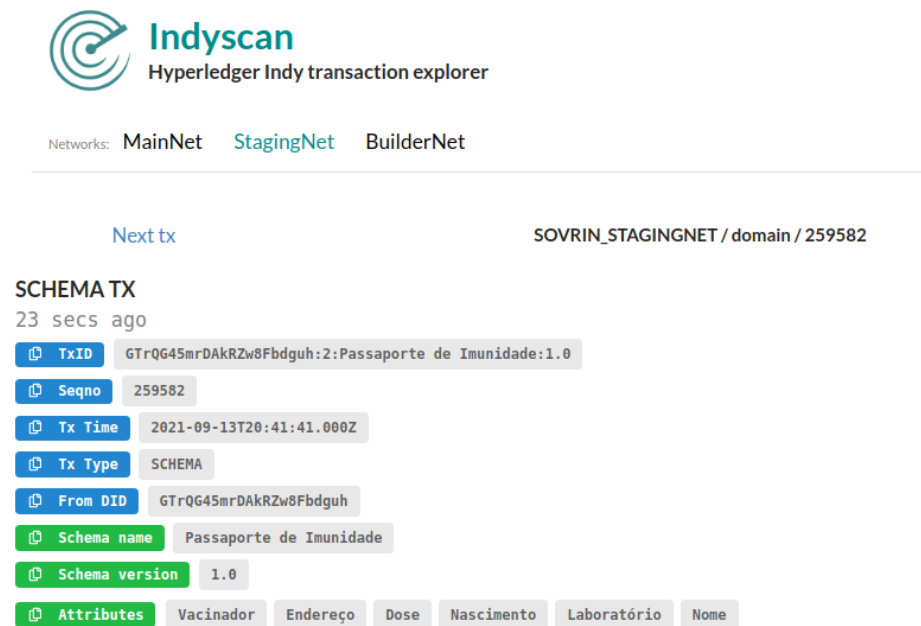


The screenshot shows the Indy Scan web application. At the top, the logo "Indyscan" is displayed with the tagline "Hyperledger Indy transaction explorer". Below the logo, there are three network selection buttons: "MainNet", "StagingNet" (which is highlighted), and "BuilderNet". The main content area shows the details of a transaction labeled "Next tx" with the identifier "SOVRIN_STAGINGNET / domain / 247993". The transaction type is "NYMTX", and it was created "33 days, 21 hours, 48 mins, 34 secs ago". The transaction details are listed as follows:

- TxID:** 1fd7b0b2ad0aa3aac066103ee8e39a52163a1ca7d841060f53a22a2d1d6be558
- Seqno:** 247993
- Tx Time:** 2021-08-10T22:47:44.000Z
- Tx Type:** NYM
- From DID:** V5qJo72nMeF7x3ci8Zv2WP
- Target DID:** GTrQG45mrDAkRZw8Fbdguh
- Verkey:** 9RpFbPMxcxCuLZweCXJh1aHZwdKxPCz6j4E5cmwH8kX4

Fonte – Indy Scan (INDYSCAN, 2021).

Figura 25 – Transação da emissão de esquema visto pelo Indy Scan.

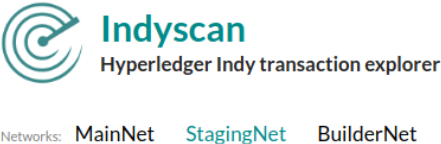


The screenshot shows the Indy Scan web application. At the top, the logo "Indyscan" is displayed with the tagline "Hyperledger Indy transaction explorer". Below the logo, there are three network selection buttons: "MainNet", "StagingNet" (which is highlighted), and "BuilderNet". The main content area shows the details of a transaction labeled "Next tx" with the identifier "SOVRIN_STAGINGNET / domain / 259582". The transaction type is "SCHEMA TX", and it was created "23 secs ago". The transaction details are listed as follows:

- TxID:** GTrQG45mrDAkRZw8Fbdguh:2:Passaporte de Imunidade:1.0
- Seqno:** 259582
- Tx Time:** 2021-09-13T20:41:41.000Z
- Tx Type:** SCHEMA
- From DID:** GTrQG45mrDAkRZw8Fbdguh
- Schema name:** Passaporte de Imunidade
- Schema version:** 1.0
- Attributes:** Vacinador, Endereço, Dose, Nascimento, Laboratório, Nome

Fonte – Indy Scan (INDYSCAN, 2021).

Figura 26 – Transação da emissão de definição de credencial.



Indyscan
Hyperledger Indy transaction explorer

Networks: MainNet StagingNet BuilderNet

Next tx SOVRIN_STAGINGNET / domain / 259583

CLAIM_DEF TX
19 secs ago

TxID	GTrQG45mrDAkRZw8Fbdguh:3:CL:259582:latest
Seqno	259583
Tx Time	2021-09-13T20:43:40.000Z
Tx Type	CLAIM_DEF
From DID	GTrQG45mrDAkRZw8Fbdguh
Schema name	Passaporte de Imunidade
Schema version	1.0
Schema ID	GTrQG45mrDAkRZw8Fbdguh:2:Passaporte de Imunidade:1.0
Schema author DID	GTrQG45mrDAkRZw8Fbdguh
Schema seqNo	259582
Schema create time	2021-09-13T20:41:41.000Z
Attributes	Vacinador Endereço Dose Nascimento Laboratório Nome

Fonte – Indy Scan (INDYSCAN, 2021).

APÊNDICE B – ARTIGO SBC

Um comprovante de vacinação baseado em Identidade Auto-Soberana, Blockchain e Provas de Zero Conhecimento

Maurício de Vasconcelos Barros

¹Sistemas de Informação – Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brasil

Abstract. *As society converges towards the online realm, new mechanisms for managing the data are needed. The outbreak of the Covid-19 pandemic in 2020 has contributed to accelerate the process of “virtualization” of society. The present work studies this problem using the Self-Sovereign Identity paradigm, where the system architecture allows the user to be the real owner of his identity. In order to understand this new model, a series of basic concepts, tools and technologies related to this work is defined, such as Digital Identity, Self-Sovereign Identity, Verifiable Credentials, Blockchain, Hyperledger, among others. After this conceptualization, a proposal and implementation of a system prototype that offers verifiable credentials to be used as proof of vaccination is carried out. Such proof uses selective disclosure techniques and proof of zero knowledge, being able to inform only a subgroup of the information contained in the credential, promoting greater security and privacy of the data contained in the credential.*

Resumo. *A medida que a sociedade vai convergindo para o reino online, novos mecanismos de gerenciamento de dados fazem-se necessários. O estourar da pandemia de Covid-19 em 2020 ajudou a acelerar o processo de “virtualização” da sociedade. O presente trabalho estuda esse problema fazendo uso do paradigma de Identidade Auto-Soberana, onde a arquitetura do sistema permite que o usuário seja o real proprietário de sua identidade. Para alcançar a compreensão desse novo modelo, primeiro é feita uma definição de uma série de conceitos basilares, ferramentas e tecnologias referentes ao tema, tais como Identidade Digital, Identidade Auto-Soberana, Credenciais Verificáveis, Blockchain, Hyperledger, entre outras. Após essa conceitualização, foi desenvolvido um protótipo de sistema que oferece credenciais verificáveis para serem usadas como um comprovante de vacinação. Tal comprovante utiliza técnicas de divulgação seletiva e provas de zero conhecimento, sendo capaz de informar apenas um subgrupo das informações contidas na credencial, promovendo maior segurança e privacidade dos dados contidos na credencial.*

1. Introdução

Nas últimas décadas o número de dados pessoais que circulam online vem crescendo de forma vertiginosa. Boa parte desses dados partem da união das redes sociais com a internet móvel. Cada vez mais setores de nossas vidas são passadas online, processo acelerado em decorrência da pandemia de Covid-19, que colocou partes da população em formas de trabalho e ensino remoto. Cada vez mais aumentamos a estatura de nossas vidas digitais.

Essas novas possibilidades nos apresentam novos desafios. O processo súbito de “virtualização” desencadeado pela pandemia, muitas vezes não ofereceu tempo e/ou treinamento necessário para a mudança para a rotina online, e se por um lado estamos mais ágeis, mais conectados e mais dinâmicos, por outro lado também estamos mais vulneráveis.

Nesse contexto emerge uma discussão a respeito da privacidade desses dados de usuários. Grandes empresas que aglomeram dados de usuários, por vezes coletam e os utilizam de forma abusiva. Exemplo disto foi o caso em 2018 da Cambridge Analytica, onde os dados de mais de cinquenta milhões de usuários do Facebook foram obtidos sem permissão e utilizados para coordenar campanhas eleitorais baseadas em perfis psicológicos extraídos dos dados obtidos [Rosenberg et al. 2018].

Exemplos dessa discussão são as recentes leis de proteção de dados que vem surgindo pelo mundo; a partir de 2020 entrou em vigor no Brasil a Lei Geral de Proteção de Dados [Brasil 2018]. Nesse novo horizonte jurídico, o cidadão ganha mais garantias sobre seus dados.

Embora a ideia de “propriedade de dados” venha ganhando força como instituição jurídica, muito ainda se carece de uma estrutura que permita um gerenciamento e controle efetivo da imensidão de dados pessoais gerados na internet todos os dias.

Para que a sociedade possa se adequar a essas novas demandas sociais, políticas e jurídicas, novos mecanismos de gestão de dados serão necessários, e para superar tais obstáculos novas ideias e tecnologias de gerenciamento devem ser pensadas. Entre esses novos mecanismos estarão novas formas de se pensar as Identidades Digitais.

Esse processo de “virtualização” transferiu as identidades “clássicas” baseadas em papel, para uma versão digitalizada, que é chamada de identidade digital [Yong et al. 2011]. O ISO 24760-1, que tem como tema segurança e privacidade para gerenciamento de identidade, coloca identidade digital como sendo “um conjunto de atributos relacionados a uma entidade”[ISO 2019]. Já em Maliki and Seigneur (2007) é definido que a identidade digital é a representação dessa entidade vinculada a um contexto específico.

Gestão de identidade é um processo para permitir a administração de uma identidade digital. Composta por políticas e tecnologias de forma a identificar entidades e permitir acesso a serviços [Ferdous et al. 2019]. O sistema que permite essa gestão de identidade é chamado de Sistema de Gerenciamento de Identidades.

Os sistemas de gerenciamento atuais são frequentemente centralizados, com a propriedade dos dados pertencendo ao provedor de identidade, tirando das mãos dos usuários a manutenção de seus dados e identidades digitais.

Identidade Auto-Soberana é um modelo de identidade digital. Segundo Allen (2016), em um sistema de Identidade Auto-Soberana o usuário deve ser central na administração da identidade, com o verdadeiro controle daquela identidade digital.

O conceito de Identidade Auto-Soberana é relevante em casos onde os dados pessoais possuem grande sensibilidade, como são os dados de saúde. Dados de pacientes são sensíveis, e exigem um cuidado especial em seu armazenamento, tratamento e compartilhamento.

Durante a pandemia de Covid-19, surgiram iniciativas de compartilhamentos de dados anonimizados que contribuam para a pesquisa do tema. Exemplos dessas iniciativas são o COVID DataSharing/BR [Fapesp 2020] no Brasil, e o United States' National Covid Cohort Collaborative (N3C) [NCATS 2021], nos Estados Unidos.

Mecanismos de compartilhamentos anonimizados e/ou de divulgações seletivas podem amparar na tomada de decisão, respeitando a privacidade dos pacientes para dados tão sensíveis como são os dados médicos.

O trabalho proposto busca investigar a tecnologia usada em sistemas de Identidade Auto-Soberana, escolhendo como caso de uso para implementação de um protótipo, a emissão e verificação de um comprovante de vacinação. A solução utiliza divulgação seletiva e provas de zero conhecimento, aumentando a privacidade dos dados do paciente.

1.1. Objetivos

1.1.1. Objetivos Gerais

O objetivo do trabalho é realizar um estudo sobre o conceito e as tecnologias envolvidas no paradigma de Identidade Auto-Soberana, buscando compreender seu funcionamento.

1.1.2. Objetivos Específicos

Os objetivos específicos são:

- Pesquisar as tecnologias e conceitos que permitam uma credencial em Identidade Auto-Soberana.
- Modelar um sistema de credenciais Auto-Soberanas com as tecnologias estudadas.
- Implementar uma prova de conceito de comprovante de vacinação por meio de uma credencial Auto-Soberana que possua divulgação seletiva e provas de zero conhecimento.

1.2. Organização

Em um primeiro momento é apresentado conceitos chaves que serão tratados, como identidades digitais e Auto-Soberana. Em seguida o trabalho perpassa diversos temas pertinentes à tecnologia abordada, como funções Hash, credenciais verificáveis, DID's, entre outros. Na sequência são abordadas as tecnologias e ferramentas descobertas, como Blockchain e os projetos Hyperledger. Por fim, é exposto a proposta e implementação realizada no presente estudo.

2. Identidades Digitais

O gerenciamento de identidades digitais vem se modificando constantemente conforme a internet e suas tecnologias vão avançando e ganhando maior importância e criticidade. A seguir o trabalho pontua alguns desses principais modelos de gerenciamento de identidades.

2.1. Modelo de Identidade Isolada

O modelo de identidade isolada foi o primeiro modelo, sendo o mais simples [Ferdous et al. 2019]. Nesse arranjo o provedor de serviços (SP - Service Provider) funcionaria também como provedor de identidade (IdP – Identity Provider). Neste modelo apenas existe o usuário e o provedor de serviço. Cada web-service que oferece algum serviço que requer autenticação, deveria implementar seu próprio sistema de gerenciamento e acesso de identidades.

O resultado deste modelo foi que os usuários tinham muitas identidades digitais espalhadas pelos diversos serviços online. Além disso, cada provedor de serviços online (web-services) tinha que arcar com os custos e dificuldades de implementação e manutenção de um sistema de gerenciamento de identidades, o que envolve a proteção contra possíveis ataques e vulnerabilidades.

2.2. Modelo de Identidade Federada

No modelo federado cada Domínio de Identidade consiste de um provedor de identidade com um ou mais provedores de serviços [Allen 2016]. O provedor de serviço utiliza o provedor de identidade para autenticação, identificação, registro e remoção de usuários. O arranjo alcançado é uma federação onde em um provedor de identidade, após identificado, o usuário pode acessar qualquer provedor de serviços que compartilhe daquele mesmo provedor de identidade [Ferdous et al. 2019].

Neste modelo os usuários não precisam possuir diversas identidades diferentes e os provedores de serviço não precisam implementar sua própria estrutura de gerenciamento de identidade. Porém o modelo federado gerou consequências não esperadas, com uma concentração imensa de dados nas mãos de poucos provedores de identidade, como Facebook, Google, Twitter e etc. Essas empresas se tornaram imensos silos de dados, se convertendo em verdadeiras “oligarquias” de provedores de identidade [Schar Dong and Custódio 2021].

Por concentrar um número muito alto de dados, esses silos se tornaram centros de atenção, chamarizes de ataques. Além disso questões como vazamentos de dados, segurança e privacidade iniciam a emergir no horizonte das questões sobre identidades digitais. Esses dados são sobre os usuários, porém os usuários não possuem esses dados; os usuários não possuem suas identidades digitais. Não somos capazes de exercer a propriedade de nossos dados.

2.3. Modelo de Identidade Auto-Soberana

A discussão sobre identidade auto-soberana inicia com a ideia que o usuário deveria possuir seus dados, possuir sua identidade digital. Embora a definição de Identidade Auto-Soberana ainda esteja em aberto, como visto em Schar Dong and Custódio (2021), Muhle et al. (2019) e Ferdous et al.(2019), em um modelo de identidade auto-soberana o usuário deve ser o soberano perante sua identidade, possuindo total controle. Os dados de identidade podem ser armazenados localmente, com os usuários, que apresentam esses dados quando necessário.

Em 2016, um texto em um blog escrito por Christopher Allen, propôs 10 princípios para identidades auto-soberanas [Allen 2016], e embora se trate de um texto

de blog, foi usado como guia e referências de diversos trabalhos que se propuseram a trabalhar com Identidade Auto-Soberana, como em Muhle et al. (2018), Ferdous et al. (2019), Kim et al. (2021), Bokkem et al. (2019), Schar Dong and Custódio (2021), entre outros.

Os dez princípios propostos por Allen são: (1) Existência – O usuário deve existir independente de qualquer provedor de serviço/provedor de identidade. (2) Controle – O usuário deve controlar suas identidades. (3) Acesso – O usuário deve sempre ter acesso a seus dados. (4) Transparência – Todos os sistemas e algoritmos devem ser transparentes para o usuário. (5) Persistência – As identidades devem ser persistidas. (6) Portabilidade – Os serviços e informações sobre a identidade do usuário deve ser transportável. (7) Interoperabilidade – As identidades devem possuir o maior alcance de uso possível entre diferentes sistemas. (8) Consentimento – O usuário sempre precisa dar seu consentimento para o uso de seus dados de identidade. (9) Minimização – Quando necessário mostrar alguma informação, sempre mostrar o mínimo possível para a realização da tarefa. (10) Proteção – Os direitos dos usuários devem ser protegidos.

Uma possível forma de implementar um sistema de gerenciamento de identidades Auto-Soberanas é com o auxílio da tecnologia Blockchain. Dessa forma, o usuário apresenta sua credencial e a parte verificadora confere no registro Blockchain sua autenticidade. Embora seja possível implementar uma Identidade Auto-Soberana sem o uso da tecnologia Blockchain, como afirma Bokkem et al. (2019), a tecnologia Blockchain é uma excelente fundação na qual é possível montar uma Identidade Auto-Soberana. Para deixar informações disponíveis de maneira pública, como esquemas de credenciais, esquemas de revogação, DIDs públicos ou chaves públicas, Blockchain funciona adequadamente, diminuindo a necessidade de pontos centralizadores.

3. Terminologia e Conceitos

De forma a melhor explicar o protótipo e a abordagem utilizada no estudo, faz-se necessário uma introdução a respeito de conceitos basilares: blockchain e mecanismos utilizados em implementações de identidades descentralizadas como DIDs e credenciais verificáveis entre outros.

3.1. Identificadores Descentralizados (DID)

Um Identificador Descentralizado, ou DID, é uma referência global única ligada a um documento DID. Seu formato é uma sequência textual composta por três partes: `esquema DID::método DID::Identificador específico` [Sporny et al. 2021]. São tipos de identificadores que permitem identidades digitais descentralizadas.

DIDs foram projetados para operar de forma independente de registros centralizados, provedores de identidades e autoridades certificadoras. Uma mesma entidade pode possuir diversos DIDs, um para cada relacionamento com outra entidade.

Todo DID é ligado a um documento DID, que é um conjunto de dados em JSON que descreve uma entidade, especificando chaves públicas, *endpoints* de serviços, etc. Essa entidade pode ser uma pessoa, um grupo, uma organização, um objeto Internet das Coisas [Sporny et al. 2021]. Todo DID é associado a uma chave verificadora.

Em um exemplo de caso de uso, um usuário acessa um site provedor de serviço e se registra, criando e enviando um novo DID nunca utilizado. O provedor de serviço

por sua vez também cria e envia um DID novo. Esses dois DIDs representam o relacionamento do usuário com o provedor de serviço. Agora, para que os dois se comuniquem, eles possuem um *endpoint* (contido do documento DID) e uma chave pública para mensagens encriptadas ponto-a-ponto. Quando o usuário retornar ao provedor de serviço, ambos trocam mensagens encriptadas e confirmam se o outro possui a chave privada para decriptar a mensagem.

3.2. Credenciais Verificáveis

Uma credencial é um conjunto de uma ou mais declarações (claims) que são feitas pela mesma entidade Emissora. Emissores fazem as afirmações em uma declaração e emitem as credenciais. Declarações (claims) são afirmações a respeito de um “sujeito”, sendo esse sujeito algo ao qual uma declaração possa ser feita. São expressas em uma relação sujeito-propriedade-valor [Sporny et al. 2019].

Credenciais podem ter metadados que descrevem propriedades como o emissor, data de validade, chave pública, revogação, etc. Credencial Verificável é um conjunto de declarações e metadados que podem provar criptograficamente o emissor por meio de uma assinatura digital [Sporny et al. 2019], provendo integridade, autenticidade e não-repúdio.

Uma Apresentação é criada para mostrar declarações para um verificador. Um verificador é o papel de quem recebe uma Credencial Verificável para verificação. Essas Apresentações Verificáveis permitem apresentar apenas um subgrupo dos atributos.

Alguns arranjos de provas de Zero Conhecimento podem criar Apresentações que provam de forma indireta a posse de uma Declaração sem revelar o dado original [Sporny et al. 2019].

Embora dois conceitos independentes, as Credenciais Verificáveis podem ser associadas a um DID por meio de um documento DID de forma a identificar um sujeito.

3.3. Provas de Zero Conhecimento

Provas de zero conhecimento, ou *Zero Knowledge Proof* (ZKP) em inglês, é um protocolo criptográfico onde um usuário é capaz de provar a outro usuário, através de computação polinomial, que ele conhece o valor de X , sem revelar qualquer outra informação além do fato que ele conhece X [Harikrishnan and Lakshmy 2019]. O resultado possível de uma prova de zero conhecimento é apenas aceitar ou rejeitar.

Zero Conhecimento é um sistema de prova interativo com dois atores, o Provedor P e o Verificador V . O Provedor é o ator que apresenta a prova, e o Verificador é aquele que a verifica. P e V devem compartilhar uma mesma entrada z , tal $(P, V)(z)$. Com essa entrada comum, P e V abrem um canal de comunicação e trocam uma sequência de mensagens, de forma que ao fim da interação o resultado deve ser $(P, V)(z) \{aceitar, rejeitar\}$ [Ibrahim 2012].

Segundo Qi e Chen (2009), um protocolo de prova pode ser considerado de zero conhecimento se possuir essas três características:

Completeness (*Completeness*): Considerando um verificador e um provedor honesto - após o cálculo da prova, se o resultado for verdadeiro, aquele que verifica pode aceitar a prova com probabilidade esmagadora de estar correto.

Eficácia (*Effectiveness*): Considerando um verificador e um provador honesto - após o cálculo da prova, se o resultado for falso, aquele que verifica pode rejeitar a prova com probabilidade esmagadora de estar correto.

Zero Conhecimento: Considerando um verificador e um provador honesto - após a verificação da prova, tendo sido a conclusão verdadeira, e estando o protocolo funcionando adequadamente, o verificador deve aceitar essa prova sem qualquer informação adicional.

Provas de Zero Conhecimento não são provas no sentido absoluto do termo, pois existe uma mínima probabilidade de um Provedor malicioso provar para um Verificador alguma declaração que seja falsa [Ibrahim 2012]. Os protocolos de zero conhecimento são pensados de forma a utilizarem técnicas para a minimização dessa probabilidade de falha da prova.

3.4. Tecnologia Blockchain

A tecnologia Blockchain permite o fim da Confiança baseada em uma autoridade central, transitando para a Confiança distribuída baseada no protocolo Blockchain; os usuários são capazes de gerenciar seus dados através de “carteiras digitais”. As carteiras digitais são peças de software com o propósito (entre outros) de armazenar conteúdos criptográficos.

Nakamoto propôs em 2008 em seu artigo o Bitcoin [Nakamoto 2008], um dinheiro eletrônico que poderia ser usado de forma peer-to-peer (P2P). Nakamoto argumenta que todo o comércio da internet baseia-se quase exclusivamente nas grandes instituições financeiras como fonte de Confiança, e propõe uma solução utilizando um servidor de timestamp distribuído peer-to-peer que é capaz de gerar provas computacionais da ordem cronológica das transações. Esse sistema utiliza o mecanismo de Proof of Work (PoW) e oferece uma proposta para resolver a vulnerabilidade do gasto-duplo (double-spending).

Essa solução ficou conhecida como Blockchain (cadeia de blocos), devido a sua estrutura de dados formada por uma lista interligada de blocos, onde cada bloco consiste de um conjunto de transações, o valor de hash do bloco anterior e um nonce.

Nessa implementação as duas estruturas principais são uma lista encadeada de hashes e uma árvore de hashes. A lista serve para manter história das transações, enquanto a árvore serve para verificação de integridade.

Nem todas as implementações de Blockchain possuem essa estrutura de dados de lista interligada, dessa forma o melhor termo a ser chamado seria Tecnologia de Registro Distribuído, ou em inglês Distributed Ledger Technology (DLT). Na bibliografia estudada os termos Blockchain e Registro Distribuído são em geral, intercambiáveis.

Esse Registro é distribuído e armazenado nos diferentes nodos em uma rede peer-to-peer (P2P), assim a segurança, imutabilidade e integridade dos dados é assegurada de forma descentralizada. Em geral, cada bloco é adicionado em um intervalo pré-definido, por meio de um algoritmo de consenso entre os nodos da rede. Esse algoritmo de consenso aliado à estrutura de hashes criptográficos, são peças chaves para garantir a integridade dos dados.

4. Hyperledger Indy

Hyperledger Indy é um projeto pertencente à comunidade Hyperledger. Hyperledger é uma comunidade open-source que tem por objetivo desenvolver frameworks, ferramentas e bibliotecas para permitir a implementação de Blockchains de nível empresarial [LINUX FOUNDATION 2015]. É uma colaboração global liderada pela Linux Foundation e inclui diversas empresas de tecnologias. Conta com diversas implementações de Blockchain para diferentes contextos.

Entre um dos projetos do Hyperledger há o HyperLedger Indy que oferece um ecossistema para gerenciamento de Identidade Auto-Soberana baseado em Blockchain [Hyperledger 2015].

4.1. Indy Distributed Ledger

O Registro Distribuído Indy é formado por dois projetos: Indy-Node e Indy-Plenum. Indy-Plenum é um Registro Distribuído de propósito geral, onde fica implementado o algoritmo de consenso, já o Indy-Node é uma especialização do Indy-Plenum, onde são implementadas as transações específicas relacionadas a identidade [Shcherbakov 2019].

O Hyperledger Indy possui o propósito de ser um Registro Distribuído específico para gerenciamento de identidade. Porém ele pode ser utilizado como um Registro de propósito geral.

O Indy-Plenum é o núcleo central onde está implementado o algoritmo de consenso, é quem escreve no Registro. O Indy-Plenum pode ser estendido através de plugins onde são implementados transações personalizadas. É o que Indy-Node faz, implementa um plugin no Indy-Plenum que adiciona as transações específicas para o gerenciamento de identidade. Assim, da mesma forma é possível adicionar novos plugins para estender o Hyperledger Indy fazendo-o um Registro de propósito geral [Shcherbakov 2019].

O Registro Distribuído do HyperLedger Indy é do tipo público permissionado [Hyperledger 2018]. Permissionado na validação pois é necessário uma permissão (um papel específico na rede) para participar da validação das transações e para escrita. E publico pois o acesso à leitura é aberto.

Nenhum dado privado é escrito na Blockchain. São escritos apenas DID's públicos, chaves públicas, esquemas de credenciais e informações sobre revogações, garantindo assim a privacidade dos dados.

As requisições de escrita necessitam de Autenticação. Toda a Autenticação é baseada em informações contidas no próprio Registro [Shcherbakov 2019]. As requisições de escrita devem ser assinadas digitalmente e essa assinatura é verificada com uma chave pública armazenada no Registro Distribuído. Requisições de leitura não necessitam nenhum tipo de Autenticação (acesso público).

A Autorização é baseada em papéis (roles) na rede (certos papéis são autorizados a fazer certas coisas), e também é dependente das informações contidas no Registro. Para requisições de leitura nenhuma Autorização é necessária (acesso público).

5. Hyperledger Aries

Hyperledger Aries é uma biblioteca pertencente à comunidade Hyperledger. Tem como objetivo prover soluções para criar, transmitir e armazenar Credenciais Verificáveis.

Aries utiliza o apoio de outra biblioteca, Hyperledger Ursa, para suporte criptográfico [Hyperledger 2020].

Aries permite interações ponto-a-ponto baseado em identidades descentralizadas, e suporta diversos registros distribuídos diferentes. Junto com Hyperledger Indy e Hyperledger Ursa, faz parte dos projetos Hyperledger voltados para implementação de sistemas de Identidade Auto-Soberana.

A biblioteca Aries possui uma camada de interface para criar, assinar e ler transações na blockchain. Fornece suporte para trocas e emissão de Credenciais Verificáveis, incluindo credenciais que utilizam as premissas de zero conhecimento, encontrados na biblioteca Ursa.

5.1. Aries Agent

Um Agente é uma peça de software com o propósito de interagir com outras entidades, via DIDs e também por outros meios. Uma instância de um Agente Aries é composta por duas partes, o agente e o controlador. O Aries Agent é o responsável por gerir as funcionalidades principais do Aries [Hyperledger 2021], incluindo interação com outros agentes, gerenciamento de armazenamento seguro, além de troca de mensagem com o controlador.

O controlador é quem provê a lógica de negócio, indicando como o agente deve responder a eventos. O Agente envia notificações de evento para o controlador, que por sua vez analisa a melhor resposta e envia mensagens administrativas para o Agente [Hyperledger 2021]. A comunicação entre os dois é feita por meio de webhooks e chamadas HTTP.

5.2. DIDComm

A comunicação entre agentes acontece por meio de um mecanismo de mensagem chamado DIDcomm (DID Communication). DIDcomm permite uma troca segura e assíncrona de mensagens encriptadas ponto-a-ponto, que geralmente são roteadas por meio de agentes Aries intermediários. A criptografia é feita pela biblioteca Hyperledger Ursa.

O mecanismo usa uma instância do método `did:peer DID method`, que faz uso de DIDs não publicados na blockchain, utilizados apenas de forma privada entre os dois agentes que se comunicam [Hyperledger 2021]. Entre os protocolos padrões definidos, que configuram um conjunto de mensagens para realizar determinada tarefa, podemos destacar:

- O protocolo “estabelecer conexão” (establish connection) que permite a conexão de dois agentes por meio de um conjunto de mensagens: o convite, a requisição de conexão e a resposta de conexão.
- O protocolo “emitir credencial” (issue credential) que permite um agente emitir uma credencial para outro agente.
- O protocolo “apresentar prova” (present proof) que permite que agentes façam requisições e recebam provas de outros agentes.

6. Passaporte Covid

Nesse contexto do recente surto de Covid-19, o paradigma de Identidade Auto-Soberana é útil. Com as tecnologias e ferramentas discutidas acima, é possível criar uma gestão de identidade que respeita a privacidade e a propriedade dos dados, por meio de mecanismos de divulgação seletiva e provas de zero conhecimento.

O período pós pandemia também gerará desafios próprios. Países tentam reabrir suas economias da forma mais segura possível, e alguns países, cidades e estados começam a requerer comprovantes de imunização, os chamados “passaporte Covid”, como o caso da cidade de São Paulo que passou a exigir tal passaporte para eventos com mais de 500 pessoas [PREFEITURA de São Paulo 2021].

Dessa forma, percebendo tal relevância, propomos a implementação de um caso de uso de um “passaporte Covid”. Uma credencial verificável, que pode ser emitida pelos órgãos de saúde e permite que o cidadão possua sua prova de vacinação no celular. Tal credencial contém dados de identificação do cidadão tais como nome, endereço, nascimento, e também dados a respeito da vacinação, como dose (primeira, segunda ou terceira), laboratório provedor da vacina e órgão vacinador.

O ecossistema se configura tal a Figura 1 mostra: Um emissor, no nosso caso, alguma entidade relacionada ao SUS, emite uma credencial verificável para o paciente vacinado. Esse paciente armazena tal credencial em uma carteira digital, e por meio dessa carteira ele é capaz de apresentar as provas de sua vacinação para as partes interessadas, no caso proposto, locais públicos, tais como aeroportos, farmácias, cinemas, casa de shows, etc. O verificador confia nas provas pois ele confia no emissor. A chave de verificação e o DID do emissor está registrado na blockchain, onde o verificador pode verificar que aquela credencial é proveniente daquele emissor.

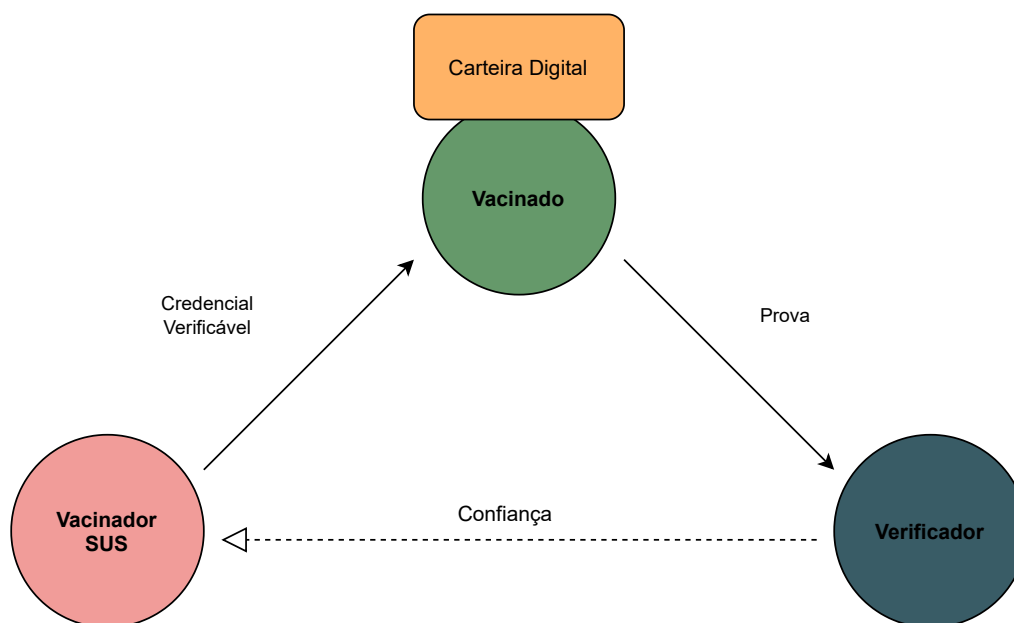


Figura 1. Papéis envolvidos no sistema proposto.

Para apresentar a prova de vacinação, serão utilizadas técnicas de divulgação seletiva e zero conhecimento, de forma que a exposição dos dados seja a mínima possível.

Para a comprovação da vacinação é apenas necessário afirmar se o número de doses é maior ou igual àquele requerido por quem verifica a vacinação. É possível também revelar dados chave necessário em situações específicas, como o nome do laboratório, ou a idade do paciente.

Essa técnica de divulgação é possível graças ao esquema de assinatura Camenisch-Lysyanskaya aplicado às credenciais, onde cada campo de um credencial verificável é assinado, assim é possível divulgá-los de forma isolada [Young 2020]. Essa assinatura também permite provas de predicado.

7. Implementação

7.1. Ferramentas utilizadas

Na parte de estudo das ferramentas existentes, ficou claro que o Hyperledger Indy é o ecossistema de código livre mais maduro voltado para implementações de Identidade Auto-Soberana, portanto é um candidato excelente para ser usado como o registro distribuído em nosso protótipo. Os esquemas de credenciais, definições de credenciais, DIDs públicos e chaves públicas ficam gravados no registro distribuído Indy.

O Hyperledger Aries é advindo do projeto Hyperledger Indy, porém se separou em um projeto próprio. Hyperledger Aries é responsável pela criação e emissão de credenciais verificáveis. O Aries opera como uma interface entre os emissores/verificadores, o registro Indy e as carteiras digitais. Tanto o Hyperledger Indy como o Hyperledger Aries utilizam a biblioteca criptográfica Hyperledger Ursa.

Para que os emissores e verificadores se comuniquem com o Hyperledger Aries, foi criado um serviço web que faz chamadas API para os agentes Aries. O modelo final do protótipo é mostrado tal qual a Figura 2.

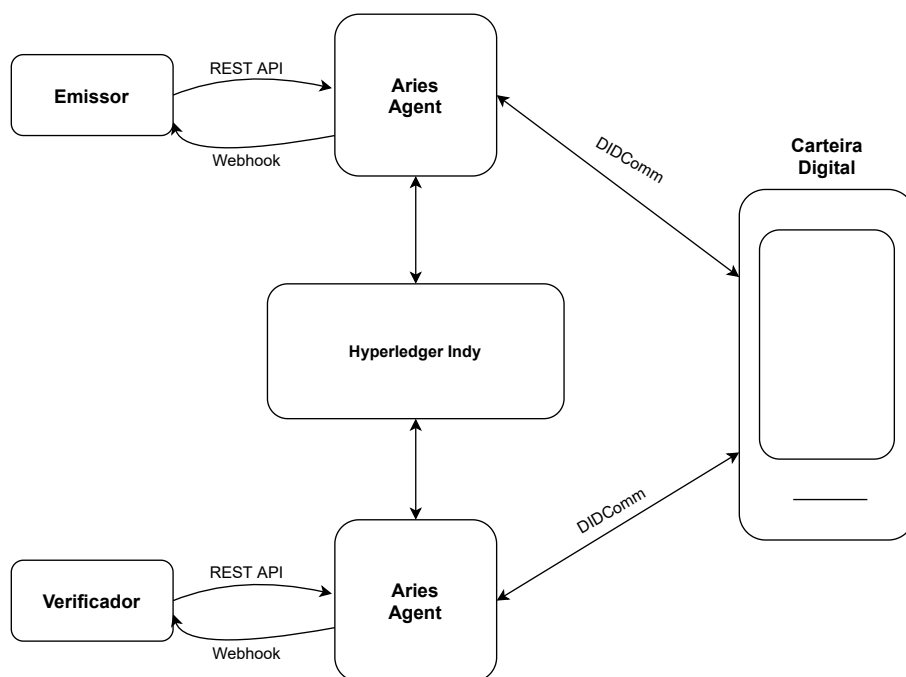


Figura 2. Arquitetura do protótipo proposto.

A rede Sovrin é regida pela Fundação Sovrin, uma fundação independente que é responsável por assegurar que o sistema de identidade Sovrin seja público e acessível globalmente [Sovrin 2021]. A rede Sovrin é pública e permissionada. É a implementação do Hyperledger Indy mais madura em produção. Possui três redes: A rede principal de produção MainNet, a rede de pré-produção StagingNet para protipação e a rede de testes BuilderNet. Por ser a principal implementação do Hyperledger Indy, optamos por utilizar a StagingNet da rede Sovrin como nosso registro distribuído, uma opção simples de utilizar. A comunicação com a rede Sovrin é feita por meio de *endpoints*.

O software Verity, produzido pela empresa Evernym [Evernym 2021], é um serviço de agente na nuvem, do tipo software-as-a-service (SaaS). Verity implementa os protocolos de comunicação do Hyperledger Aries. O software Verity é uma maneira simples de implementar um agente Aries, pois funciona como um servidor onde enviamos chamadas REST e ele retorna Webhooks. Esse servidor permite ao desenvolvedor se comunicar por DIDComm com as carteiras digitais e também com o registro distribuído. Por essas facilidades, optamos por utilizar o servidor Verity como nosso agente Aries.

Por fim, A carteira digital para mobile Connect.me [Evernym 2018], também produzida pela empresa Evernym, oferece compatibilidade com as ferramentas acima citadas, uma solução gratuita que permite conexões únicas baseadas em DIDs. No contexto do protótipo, as credenciais verificáveis emitidas devem ser armazenadas em carteiras digitais.

7.2. Protótipo

Munido das ferramentas acima citadas, com a rede Sovrin operando como o registro distribuído Hyperledger Indy, o servidor da Verity tratando das comunicações DIDComm oferecidas pelo Hyperledger Aries, e finalmente a carteira Connect.me para armazenamento das credenciais, configura todas as partes para que o protótipo de uma credencial verificável Passaporte Covid possa ser implementada.

A última etapa desse ecossistema foi a criação de serviços web representando tanto o emissor como o verificador, para realizar as chamadas REST e comunicar-se com o restante do sistema. O emissor e o verificador foram realizados por meio de HTML e Javascript. Com esses sistema é possível montar uma credencial verificável para provar a vacinação, como descrito a seguir.

A operação do protótipo segue o seguinte fluxo:

- Emissor registra DID no Indy.
- Emissor registra Esquema de Credencial no Indy.
- Emissor registra Definição de Credencial no Indy.
- Emissor conecta-se com a carteira digital do paciente.
- Emissor emite credencial que fica armazenada na carteira digital.
- Verificador conecta-se a carteira digital do paciente.
- Verificador envia requisição de prova para a carteira do paciente.
- Paciente compartilha a prova de vacinação.

O primeiro passo a ser feito é registrar um DID para o emissor no registro distribuído Indy da Sovrin, no protótipo tal DID pertence a alguma entidade vinculada ao SUS. Esse registro é realizado por meio de chamadas API, assim ao clicar no botão "Cadastrar Emissor", é gerado um par de chaves para DID e enviado por meio de chamadas

REST para a interface do Hyperledger Aries, que por sua vez o envia para a rede Sovrin onde é registrado de forma permanente no registro distribuído.

Tendo sido o emissor devidamente registrado na rede Sovrin, ele torna-se capaz de fazer novas transações na rede, como emitir um modelo de esquema de credencial que será utilizado. O esquema de credencial do protótipo conta com os seguintes campos: nome, endereço, nascimento, laboratório, dose e vacinador.

Após a emissão do esquema, seguindo o fluxo, é necessário registrar também no registro distribuído a definição de credencial. Nessa etapa, é associada essa definição de credencial ao DID do emissor, em nosso caso o vacinador, vinculado ao SUS.

Tendo o emissor sendo registrado na rede Sovrin, emitido seu esquema de credencial e também sua definição de credencial, está ele devidamente preparado para emitir de fato a credencial verificável com o comprovante de vacinação. Primeiramente o emissor inicia um relacionamento com a carteira digital do paciente vacinado. O sistema do emissor gera um QR Code com o convite para o relacionamento, que é lido pelo celular do paciente.

Após o paciente ler e aceitar a conexão, um DID é gerado que representa o relacionamento entre o emissor e o paciente. Estando os dois conectados, o emissor pode emitir para o paciente a credencial.

De forma a receber a credencial, o paciente deve aceitar a credencial em seu celular. Agora o paciente possui sua credencial verificável que demonstra a vacinação de sua primeira dose. Já é possível oferecer tais provas para um possível verificador.

De forma análoga ao emissor, o primeiro passo do verificador é conectar-se com a carteira digital do paciente, operação realizada da mesma forma que com o emissor, primeiro é gerado um convite com o QR Code e o paciente deve escanear esse convite a aceitar a conexão.

Com o verificador conectado ao paciente, já é possível para o verificador fazer a requisição da prova de vacinação.

Tal requisição de prova chegará como uma notificação no celular do portador da credencial, que deve aceitar a requisição (para provar a vacinação) para que ela possa ser enviada para o verificador.

Como contraexemplo, foi requisitado uma prova de verificação da terceira dose da vacina, ou seja, uma requisição de prova onde o valor do campo "dose" deverá ser maior ou igual a três. Caso o portador da credencial não possua tal valor, não é possível compartilhar tal prova.

7.3. Resultados

Com esse arranjo foi possível concluir o protótipo de uma credencial verificável para um comprovante de vacinação "Passaporte Covid". O emissor se cadastrou na rede Sovrin, emitiu um esquema de credencial e uma definição de credencial, por fim emitiu a credencial verificável contendo o comprovante de vacinação.

O portador da credencial por sua vez, aceitou a credencial que ficou armazenada em uma carteira digital em seu celular, podendo apresentá-la quando necessário.

Todo o arranjo permite divulgação seletiva e provas de zero conhecimento. Foi possível comprovar a vacinação do portador da credencial, mostrando apenas o nome do laboratório e se o número de doses é maior ou igual àquele requerido pelo verificador. Tal arranjo garante privacidade de todos os outros dados do portador que não são necessários para provar a vacinação.

Em um cenário onde o comprovante de vacinação seja em formato de papel, todos os dados do portador seriam expostos, tornando uma verificação mais invasiva.

8. Considerações Finais e Trabalhos Futuros

8.1. Considerações Finais

O desenvolvimento do presente estudo possibilitou um levantamento de temas, ferramentas e tecnologias que permitem o uso do modelo de Identidade Auto-Soberana. Utilizando a ferramenta Hyperledger Indy para o registro distribuído possibilita a diminuição da centralização. A rede Indy fornece a capacidade de oferecer confiança. O emissor (das credenciais) tem seu DID e sua chave de verificação registrados na Blockchain, que são checados pelo verificador. Enquanto a rede distribuída estiver funcionando, o registro continuará disponível.

Os protocolos do Hyperledger Aries fornecem interface entre diferentes atores, emissão e gerenciamento de credenciais verificáveis, se comunica com a carteira digital e com o registro distribuído. Suas interações sempre amparadas pelas bibliotecas criptográficas do Hyperledger Ursa.

Essa tríade de projetos, Indy, Aries e Ursa oferecem em conjunto um ecossistema onde diversas implementações de modelos de Identidade Auto-Soberana podem existir. Esses novos modelos trazem maior privacidade, segurança e propriedade para os dados de usuários.

Com sucesso, utilizando esse modelo, o presente trabalho foi capaz de montar um sistema de emissão e verificação de credenciais, amparado pela tecnologia Blockchain e funções criptográficas. Tal protótipo gerou um certificado de vacinação que garante mecanismos de divulgação seletiva e provas de zero conhecimento. Este certificado, que é custodiado pelo próprio vacinado, garante a comprovação da vacinação com grande nível de privacidade de seus dados, diferindo-se de outros modelos de identidade.

Apesar de possíveis polêmicas a favor ou contra os ditos “passaportes de vacinação”, credenciais verificáveis, com divulgação seletiva, tornam o seu uso menos invasivo. Dessa forma, aliviando o peso das inúmeras mudanças que o mundo inteiro vem realizando para se adaptar à pandemia e seus efeitos.

A medida que cada vez mais pessoas vão percebendo a importância de um tratamento adequado de seus dados digitais, o tema de privacidade ganhará mais importância. Provavelmente ainda teremos um longo caminho para aperfeiçoar o trato de nossos dados. Esse caminho perpassará modelos de gestão de identidades tais como o de Identidade Auto-Soberana.

No futuro que se aproxima, novas políticas, mecanismos e paradigmas de gerenciamento de dados serão criados, provavelmente novas legislações, conforme passamos mais tempo de nossas vidas no mundo online. Paradigmas como a Identidade Auto-

Soberana farão parte desse futuro, suas tecnologias como Blockchain e suas ferramentas como Hyperledger Indy e Aries, provavelmente crescerão e ficarão mais robustas conforme vamos nos adaptando a novas realidades digitais. O futuro é digital, e nossos dados são e devem ser nossos.

8.2. Trabalhos Futuros

Podemos citar como possíveis trabalhos futuros:

- Aperfeiçoamento do protótipo, adicionando algum tipo de revogação e tornando a interface gráfica o mais simples possível. Gerar *Templates* de requisição de prova pré-feitos.
- Realização de testes de rede, verificar as capacidades de emissão do sistema.
- Expandir o modelo de credencial para ser utilizado de forma genérica em outros casos de uso.

Referências

- Allen, C. (2016). The path to self-sovereign identity. Disponível em: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>. Acesso em: 04 abr. de 2021.
- Bokkem, D. V., Hageman, R., Koning, G., Nguyen, L., and Zarin, N. (2019). Self-sovereign identity solutions: The necessity of blockchain technology.
- Brasil (2018). Lei geral de proteção de dados pessoais (lgpd).Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil-03/-ato2015-2018/2018/lei/113709.htm>. Acesso em:27 set. de 2021.
- Evernym (2018). Connect.me. Disponível em: <https://www.connect.me/>. Acesso em: 10mai. de 2021.
- Evernym (2021). Building ssi solutions has never been easier. Disponível em: <https://www.evernym.com/products/#credentials>. Acesso em: 22 mai. de 2021
- Fapesp (2020). Fapesp covid-19 datasharing/br. Disponível em: <https://repositoriodatasharingfapesp.uspdigital.usp.br/>. Acesso em: 8 set. de 2021.
- Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. (2019). In search of self-sovereignidentity leveraging blockchain technology.IEEE Access, 7:103059–103079.
- Harikrishnan, M. and Lakshmy, K. (2019). Secure digital service payments using zeroknowledge proof in distributed network. In2019 5th International Conference onAdvanced Computing Communication Systems (ICACCS), pages 307–312.
- Hyperledger (2015). Hyperledger indy. Disponível em: <https://www.hyperledger.org/use/hyperledger-indy>. Acesso em: 03 mai. de 2021
- Hyperledger (2018). Welcome to hyperledger indy node's documentation. Disponível em: <https://hyperledger-indy.readthedocs.io/projects/node/en/latest/index.html>. Acesso em: 03mai. de 2021.
- Hyperledger (2020). Hyperledger aries. Disponível em: <https://github.com/hyperledger/aries>. Acesso em: 16 ago. de 2021.
- Hyperledger (2021). Becoming a indy/aries developer. Disponível em: <https://github.com/hyperledger/aries-cloudagent-python/tree/main/docs/GettingStartedAriesDev>. Acesso em: 11 jun. de 2021.
- Ibrahim, M. K. (2012). Modification of diffie-hellman key exchange algorithm forzero knowledge proof. In2012 International Conference on Future CommunicationNetworks, pages 147–152.
- ISO (2019). Iso/iec 24760-1:2019(en) it security and privacy — a framework for identitymanagement — part 1: Terminology and concepts. Disponível em:<https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en>. Acesso em: 12 jun. de 2021

- Kim, B. G., Cho, Y.-S., Kim, S.-H., Kim, H., and Woo, S. S. (2021). A security analysis of blockchain-based did services. *IEEE Access*, 9:22894–22913.
- Linux Foundation (2015). Hyperledger. Disponível em: <https://www.hyperledger.org/>. Acesso em: 03 mai. de 2021.
- Maliki, T. E. and Seigneur, J.-M. (2007). A survey of user-centric identity management technologies. In *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, pages 12–17.
- Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Disponível em: <http://arxiv.org/abs/1807.06346>. Acesso em: 27 set. de 2021
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 04 abr. de 2021
- NCATS (2021). National covid cohort collaborative (n3c). Disponível em: <https://ncats.nih.gov/n3c>. Acesso em: 8 set. de 2021
- Prefeitura de São Paulo (2021). Passaporte da vacina será solicitado para acesso a eventos a partir desta quarta-feira em São Paulo. Disponível em: <https://www.capital.sp.gov.br/noticia/passaporte-da-vacina-sera-solicitado-para-acesso-a-eventos-a-partir-desta-quarta-feira-em-sao-paulo>. Acesso em: 8 set. de 2021
- Qi, M. and Chen, B. (2009). Construction of safe patent trading platform based on zero-knowledge proof. In *2009 Asia-Pacific Conference on Information Processing*, volume 2, pages 627–630.
- Rosenberg, M., Confessore, N., and Cadwalladr, C. (2018). How trump consultants exploited the facebook data of millions. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em: 3 set. de 2021.
- Schardong, F. and Custódio, R. (2021). Self-sovereign identity: A systematic map and review. Disponível em: <https://arxiv.org/abs/2108.08338>. Acesso em: 20 set. de 2021
- Shcherbakov, A. (2019). Hyperledger indy public blockchain node with alexander sh-cherbakov. Disponível em: <https://www.youtube.com/watch?v=UJbJRqur4ng>. Acesso em: 15 mai. de 2021.
- Sovrin (2021). Sovrin. Disponível em: <https://sovrin.org/>. Acesso em: 22 mai. de 2021.
- Sporny, M., Longley, D., and Chadwick, D. (2019). Verifiable credentials data model 1.0. Disponível em: <https://www.w3.org/TR/vc-data-model/>. Acesso em: 26 ago. de 2021.
- Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., and Allen, C. (2021). Decentralized identifiers (dids) v1.0. Disponível em: <https://www.w3.org/TR/did-core/>. Acesso em: 26 ago. de 2021.

- Yong, J., Tiwari, S., Huang, X., and Jin, Q. (2011). Constructing robust digital identity infrastructure for future networked society. In Proceedings of the 2011 15th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pages 570–576.
- Young, K. (2020). Verifiable credentials flavors explained. Disponível em: <https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf>. Acesso em: 25 set. de 2021