Cariniana
Rede Brasileira de Serviços de Preservação Digital

# InterPARES Trust Project Report

## Modelo para Preservação da Confiabilidade de Registros Digitais Assinados (TRUSTER Preservation Model)

Brasília, DF

Outubro de 2025

ibict
Instituto Brasileiro de Informação em Ciência e Tecnologia

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

# InterPARES Trust Project Report

## Modelo para Preservação da Confiabilidade de Registros Digitais Assinados

## (TRUSTER Preservation Model)

**Documento Original:** *Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31)*

**Versão Original:** 1.3 (8 de março de 2018)

**Autor Original:** InterPARES Trust Project


**Equipe de Pesquisa**

**Coordenador:** Hrvoje Stančić (FHSS)

**Membro da Equipe:** - Göran Almgren (Enigio Time AB) - Hans Almgren (Enigio Time AB) - Natasha Khramtsovsky (Electronic Office Systems LLC) - Victoria Lemieux (UBC) - Željko Mikić (TechEd) - Elis Missoni (FINA) – Mats Stengård (Enigio Time AB)

**Assistentes de Pesquisa FHSS:** Andro Babić, Nikola Bonić, Vladimir Bralić, Hrvoje Brzica, Magdalena Kuleš, Anabela Lendić, Ksenija Lončarić, Ivan Slade Šilović, Ana Stanković, Ira Volarević

**Tradução para o Português**

**Equipe de Tradução**

• Neide A. D. De Sordi

• José Alexandre C. Vasco

• Márcia Teixeira Cavalcanti

**Coordenação**

**• Coordenador do Comitê PreservIA:** Charlley Luz

**• Coordenador da Rede DRÍADE:** Miguel Angel Mardero Arellano



DRÍADE - Rede de Repositórios Digitais Confiáveis

Rede Cariniana - Rede Brasileira de Serviços de Preservação Digital

IBICT - Instituto Brasileiro de Informação em Ciência e Tecnologia

Brasília, DF

Outubro de 2025

**Sobre o Documento Original**

O presente documento é a tradução do relatório final do projeto EU31 do InterPARES Trust Project, intitulado "*Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model)*".

**Sobre a Tradução**

Esta tradução foi realizada de forma fiel ao documento original em inglês, preservando a estrutura, o conteúdo técnico e a terminologia especializada. Foram incluídas notas de rodapé quando necessário para facilitar a compreensão no contexto brasileiro.

O objetivo desta tradução é disponibilizar para a comunidade brasileira de preservação digital um importante recurso sobre modelos de preservação de registros digitais assinados, contribuindo para o desenvolvimento de políticas e práticas de preservação digital no país.

**Direitos e Licenciamento**



**Como Citar Esta Tradução:** STANČIĆ, Hrvoje et al. Modelo para Preservação da Confiabilidade de Registros Digitais Assinados (TRUSTER Preservation Model). Tradução de Neide A. D. De Sordi, José Alexandre C. Vasco e Márcia Teixeira Cavalcanti. Coordenação de Charlley Luz e Miguel Angel Mardero Arellano. DRÍADE, Rede Cariniana, IBICT, outubro 2025.

# Relatório do Projeto InterPARES Trust1

| | |
|---|---|
| **Título e código:** | **Modelo para preservação da confiabilidade de registros digitais assinados digitalmente, com carimbo de tempo e/ou selados (modelo de preservação TRUSTER) (EU31)** |
| **Tipo de documento:** | Relatório final |
| **Status:** | Versão final Versão: 1.3 |
| **Domínio de pesquisa:** | Controle |
| **Data de envio:** | 3 de fevereiro de 2018 |
| **Última revisão:** | 8 de março de 2018 |
| **Autor:** | InterPARES Trust Project |
| **Escritor:** | Hrvoje Stančić |
| **Equipe de pesquisa:** | Göran Almgren (Enigio Time AB), Hans Almgren (Enigio Time AB), Natasha Khramtsovsky (Electronic Office Systems LLC), Victoria Lemieux (UBC), Željko Mikić (TechEd), Elis Missoni (FINA), Hrvoje Stančić (FHSS), Mats Stengård (Enigio Time AB) FHSS GRAs: Andro Babić, Nikola Bonić, Vladimir Bralić, Hrvoje Brzica, Magdalena Kuleš, Anabela Lendić, Ksenija Lončarić, Ivan Slade Šilović, Ana Stanković, Ira Volarević |

1 Os termos '*TRUSTER*', '*Trust*' e "TrustChain" foram mantidos como no original por constituírem nomes próprios de modelos e projetos específicos (TRUSTER Preservation Model, InterPARES Trust Project e o Modelo *TrustChain* respectivamente), não sendo, portanto, traduzidos para o português.

**Controle de Documentos**

| Histórico de Versões | | | |
|---|---|---|---|
| Version | Date | By | Version notes |
| 0.1 H. | | H. Stančić | Versão inicial |
| 0.3 | 16.12.2017 | Membros da equipe | Versão de trabalho |
| 0.4 | 17.12.2017 | Membros da equipe | Versão de trabalho |
| 0.5 | 19.12.2017 | Membros da equipe | Versão de trabalho |
| 0.6 | 27.12.2017 | H. Stančić | Versão de trabalho |
| 1.0 | 07.01.2018 | H. Stančić | Versão para consulta no nível da União Europeia 31 |
| 1.1 | 12.01.2018 | V. Bralić, N. Khramt-sovsky, M. Stengård | Sugestões de melhoria |
| 1.2 | 03.02.2018 | H. Stančić | Versão final |
| 1.3 | 08.03.2018 | H. Stančić | Pequenas correções |

# Conteúdo

## 1. Resumo

A preservação a longo prazo de registros digitais que são assinados digitalmente ou possuem um selo digital anexado é um desafio para a profissão arquivística. Esses registros digitais não são fáceis de preservar, não apenas devido aos constantes avanços tecnológicos, mas também porque os certificados nos quais se baseiam têm duração limitada. Além das três abordagens bem conhecidas para a preservação de registros assinados digitalmente, a saber: 1) preservar as assinaturas digitais, 2) eliminar as assinaturas e 3) registrar o rastro das assinaturas como metadados, esta pesquisa propôs o modelo de uma quarta abordagem – registrar a validade da assinatura digital em uma blockchain[2].

A equipe levantou 13 questões de pesquisa, correspondentes aos três objetivos e metas do estudo. Os objetivos do estudo foram: 1) abordar uma questão arquivística importante sobre a preservação de registros digitais na nuvem utilizando novos conceitos tecnológicos, como blockchain, 2) construir um modelo que sugira como preservar a confiabilidade dos registros digitais com assinaturas digitais, certificados, carimbos de tempo ou selos adicionados a eles, e 3) investigar as possibilidades de revalidação de assinaturas digitais expiradas, nova assinatura periódica de registros digitais ou renovação de carimbos de tempo, adição de carimbos de tempo arquivísticos, inclusão de provas adicionais (com carimbo de tempo) de existência, etc. As metas do estudo foram: 1) alcançar resultados que possam ser usados para elaborar e/ou melhorar estruturas regulatórias, 2) alcançar resultados que possam ser usados para elaborar e/ou melhorar políticas e procedimentos organizacionais internos, e 3) alcançar resultados relevantes para a organização e o desenvolvimento de serviços arquivísticos confiáveis baseados na ingestão de registros confiáveis[3].

Para atingir os objetivos e metas estabelecidos e responder às questões de pesquisa, o estudo foi dividido em cinco fases, às vezes sobrepostas, ao longo de 19 meses (março de 2016 – setembro de 2017): 1) revisão da literatura relevante, 2) desenvolvimento de três estudos de caso, 3) teste de vários casos de uso de gestão documental e preservação arquivística, 4) desenvolvimento do modelo para preservação da validade de registros assinados digitalmente e com carimbo de tempo, e 5) redação do relatório final.

Os estudos de caso (CS, do inglês *Case Study*) mostraram que, nas três instituições pesquisadas, que possuem registros de fundos de aposentadoria assinados digitalmente (CS1), registros fiscais eletrônicos assinados digitalmente (CS2) e registros médicos assinados digitalmente, contratos de fornecedores e de compras, decisões políticas oficiais e atas de reuniões (CS3), ainda não foram realizadas ações de preservação digital. Além disso, constatou-se que há registros com assinaturas digitais expiradas ou prestes a expirar, que esses registros são vitais para certos processos importantes envolvendo cidadãos e que há necessidade de desenvolvimento de estratégias e políticas de preservação digital para garantir a validade das assinaturas digitais.

A equipe de pesquisa desenvolveu o modelo chamado "*Solução TRUSTER VIP (Preservation of Validity Information): TrustChain*". O *TrustChain* foi modelado como uma solução baseada em blockchain que permite que instituições arquivísticas (ou outras com necessidades semelhantes) evitem a necessidade de reassinar periodicamente (ou adicionar carimbos de tempo) a todos os seus registros arquivados e assinados digitalmente. O *TrustChain* alcança isso verificando a validade da assinatura do registro no momento da

---

2 Para casos de uso específicos, também foi recomendada a consideração da possibilidade de transferir as obrigações de preservação dos registros originais assinados digitalmente para um banco de dados confiável formado a partir desses registros, descartando os registros originais (já inutilizáveis). Tal transferência exige mudanças na legislação e/ou regulamentações e pode necessitar de aprovação pelos Arquivos Nacionais.

3 Alternativamente, os serviços de uma terceira parte confiável pode ser utilizada em vez de (ou como provedores de) uma solução baseada em blockchain. Em qualquer caso, a solução deve ser respaldada por legislação e/ou regulamentações correspondentes.

ingestão e, se válida, registrando o *hash*4,5 da assinatura (e alguns metadados) na blockchain. A validade da assinatura é verificada por todas ou, se o número for suficientemente alto, por algumas (maioria qualificada) das instituições participantes da rede distribuída de instituições confiáveis interconectadas. Se a assinatura for considerada válida, a informação é armazenada permanentemente na blockchain do *TrustChain*, ou seja, no livro-razão distribuído6.

Prevemos que o *TrustChain*, uma solução VIP baseada em blockchain, seja mantido por uma aliança internacional de instituições arquivísticas.

Além do questionário do estudo de caso encontrado no Apêndice 1, a pesquisa produziu três relatórios de estudos de caso e uma bibliografia sobre blockchain como produtos separados, bem como a lista de termos e definições relacionados a blockchain que foram incluídos no banco de dados de terminologia do InterPARES Trust.

---

4 [N. do T.]. Opta-se por manter o termo “hash”, embora “resumo criptográfico” seja o equivalente consagrado em português, por três razões principais: (i) precisão de uso no contexto de blockchain, em que “hash” designa tanto a função quanto o valor resultante, enquanto “resumo criptográfico” costuma enfatizar apenas o artefato; (ii) interoperabilidade terminológica com a literatura técnica internacional, padrões, APIs e ferramentas, que adotam “hash” de forma quase universal; e (iii) economia e clareza estilística, já que “hash” é curto, amplamente reconhecido na comunidade técnica lusófona e evita ambiguidades que podem surgir com alternativas menos comuns como “função/código/valor de dispersão

5 [N. do T.]. Refere-se a uma função matemática que transforma dados de qualquer tamanho em uma sequência fixa de caracteres, geralmente números e letras.

6 Blockchain é uma tecnologia de registro distribuído (*Distributed Ledger Technology - DLT*) que funciona como um banco de dados compartilhado, replicado e sincronizado em uma rede de múltiplos participantes. As transações são registradas de forma imutável e gerenciadas de maneira descentralizada, eliminando a necessidade de um intermediário central. WORLD ECONOMIC FORUM. Evolution of Non-Fungible Tokens. Geneva: World Economic Forum, 2023. Disponível em: https://www3.weforum.org/docs/WEF_Evolution_of_NFTs_2023.pdf. Acesso em: 15 ago. 2025.

## 2. Apresentação

O relatório **TRUSTER Preservation Model (EU31)**, desenvolvido no âmbito do projeto **InterPARES Trust (ITrust, 2012–2019)**, é uma iniciativa multinacional e interdisciplinar dedicada a investigar questões de confiança e confiabilidade de registros e dados em ambientes digitais.

O ITrust teve como objetivo formular fundamentos teóricos e metodológicos capazes de apoiar o desenvolvimento de políticas, procedimentos, regulamentações, padrões e legislações em escala local, nacional e internacional. A meta central foi assegurar a confiança pública, sustentada em boa governança, economia digital sólida e memória digital persistente.

A rede de pesquisa que compôs o ITrust envolveu mais de cinquenta universidades e organizações públicas e privadas na América do Norte, América Latina, Europa, África, Austrália, Nova Zelândia e Ásia. Reuniram-se especialistas em ciência da informação arquivística, gestão documental, diplomática, direito, tecnologia da informação, comunicação e mídia, jornalismo, comércio eletrônico, informática em saúde, cibersegurança, governança da informação, forense digital, engenharia da computação e políticas de informação.

A tradução para o português deste relatório foi realizada por pesquisadores do Grupo de Estudo PreservIA (Inteligência Artificial na Preservação Digital - PreservIA), que integra a DRÍADE, criada pelo Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) como parte das iniciativas da Rede Cariniana. A versão brasileira busca ampliar o acesso a esse modelo de preservação confiável, promovendo o diálogo com especialistas, gestores e instituições nacionais.

Esperamos que a tradução incentive a adoção do Trust Model no Brasil. Como exemplo, destacamos algumas iniciativas recentes que dialogam diretamente com seus princípios:

- **Autenticidade em documentos oficiais:** em 2025, o Governo Federal oficializou o uso de blockchain para certificação de data e hora, dando continuidade à experiência iniciada em 2021 pelo Instituto Nacional de Tecnologia da Informação (ITI) com o carimbo de tempo da ICP-Brasil.
- **Educação e preservação da memória acadêmica:** no mesmo ano, o Ministério da Educação, em parceria com a Rede Nacional de Pesquisa (RNP) e a empresa LedgerTec, consolidou a emissão de diplomas universitários em blockchain, alcançando mais de 360 mil documentos e envolvendo mais de 190 instituições de ensino superior.

Esses exemplos ilustram, na prática, o papel de um Trust Model: assegurar a autenticidade, a integridade e a confiabilidade das informações digitais sem depender de verificações manuais ou de intermediários centralizados. Nesse contexto, a confiança é garantida por mecanismos técnicos — criptografia, redes distribuídas e validações automatizadas — que tornam a informação verificável de forma transparente, persistente e resistente a fraudes.

Essas iniciativas convergem com os objetivos do TRUSTER: construir uma infraestrutura confiável de preservação digital de longo prazo, que una governança, tecnologia de registro distribuído e regulamentação robusta. Assim, esta tradução não apenas aproxima o leitor brasileiro das boas práticas internacionais, como também estimula a integração entre avanços locais e modelos globais, reforçando o compromisso mútuo com a autenticidade, a segurança e a confiabilidade da memória digital.

## 3. Equipe de Pesquisa

**Pesquisador Principal:**

- Dr. Hrvoje Stančić, professor associado, Faculdade de Humanidades e Ciências Sociais (FHSS), Universidade de Zagreb, Croácia

**Pesquisadores do Projeto:**

- Göran Almgren, Enigio Time AB, Estocolmo, Suécia
- Hans Almgren, Enigio Time AB, Estocolmo, Suécia
- Dr. Natasha Khramtsovsky, Electronic Office Systems LLC, Moscou, Rússia
- Dr. Victoria Lemieux, professora associada, Universidade da Colúmbia Britânica (UBC), Vancouver, Canadá
- Željko Mikić, TechEd Consulting Ltd., Zagreb, Croácia
- Elis Missoni, Agência Financeira – FINA, Zagreb, Croácia
- Mats Stengård, Enigio Time AB, Estocolmo, Suécia

**Assistentes de Pesquisa Graduados:**

- Andro Babić, março de 2016 – presente (FHSS)
- Nikola Bonić, março de 2016 – outubro de 2016
- Vladimir Bralić, março de 2016 – presente
- Hrvoje Brzica, março de 2016 – presente
- Magdalena Kuleš, junho de 2016 – presente
- Anabela Lendić, março de 2016 – presente
- Ksenija Lončarić, março de 2016 – abril de 2016
- Ivan Slade Šilović, agosto de 2016 – presente
- Ana Stanković, março de 2016 – abril de 2016
- Ira Volarević, março de 2016 – outubro de 2016

# 4. Contexto

## 4.1 Registros digitais no contexto da preservação a longo prazo

Atualmente, os registros digitais podem ser criados de duas maneiras: podem ser digitalizados a partir de registros em papel existentes ou nato digital. A digitalização, no sentido mais amplo, representa a transformação de um sinal analógico em uma forma digital correspondente e, em um sentido mais restrito, refere-se à transformação de diferentes materiais em uma forma digital, convertendo-os em código binário no formato de um arquivo de computador7. A digitalização divide o conceito de preservação em duas partes: a preservação do conteúdo informacional ou da informação registrada em um documento e a preservação do objeto físico, ou seja, o meio que carrega a informação. O conteúdo informacional é digitalizado e salvo separadamente do objeto físico. (Stančić, Digitization of documents, 2000). É importante destacar que todo registro preservado digitalmente deve manter intactas suas características de autenticidade, confiabilidade, integridade e usabilidade. (ISO 15489-1:2016 Informação e documentação – Gestão de registros – Parte 1: Conceitos e princípios, 2016). A confiabilidade de um registro refere-se à sua precisão, confiabilidade e autenticidade. (InterPARES Trust Terminology Database).

O arquivamento e a preservação representam um desafio único devido à natureza de longo prazo dessas atividades. O problema da preservação e manutenção a longo prazo de informações digitais pode ser interpretado como a necessidade de preservar registros de forma que a tecnologia em que se baseiam não se torne obsoleta. Objetos digitais exigem manutenção constante e contínua e dependem de um ecossistema complexo de hardware, software, padrões e regulamentações legais que estão em constante mudança, sendo alterados ou substituídos. Quando comparados aos registros analógicos, os registros digitais enfrentam um risco maior de deterioração, principalmente devido ao rápido ritmo de desenvolvimento da tecnologia da informação. A preservação de registros digitais vai muito além da preservação de um arquivo de computador – o objetivo é permitir o acesso ao conteúdo enquanto se garante que suas características importantes sejam preservadas.

## 4.2 Registros assinados digitalmente

O resultado dos negócios eletrônicos e da comunicação digital é a criação de um número cada vez maior de documentos e registros digitais, que podem conter assinaturas digitais ou selos digitais anexados a eles. Por isso, é necessário analisar os desafios da preservação a longo prazo desses registros digitais.

Embora tecnicamente semelhantes, a diferença entre assinaturas digitais8 e selos digitais é que a assinatura digital pode ser associada apenas a uma pessoa física, e a chave de assinatura deve estar sob o controle exclusivo do signatário com o objetivo de assinar. Já o selo digital pode ser associado apenas a uma pessoa jurídica, e a chave de assinatura deve estar sob o controle exclusivo do processo que atribui o selo, com o objetivo de garantir a integridade e a origem. (What is an electronic seal?; eIDAS, 2014).

Para serem preservados a longo prazo, os registros assinados digitalmente também devem possuir as características básicas de autenticidade, confiabilidade, integridade e usabilidade, o que exige uma abordagem mais complexa de preservação em comparação com registros digitais que não são assinados ou selados digitalmente. Assim como há uma diferença entre a preservação de curto e longo prazo de re-

---

7 Enciclopédia Croata (Instituto de Lexicografia Miroslav Krleža, 2017)

8 Os termos assinatura eletrônica e assinatura digital são frequentemente usados de forma intercambiável para significar a mesma coisa. No entanto, neste relatório, o termo assinatura eletrônica será usado quando nos referirmos às assinaturas nas quais a identidade do signatário não pode ser verificada, enquanto o termo assinatura digital será usado quando nos referirmos às assinaturas em que a Autoridade Certificadora (AC) confirma a identidade do signatário (exceto nas citações onde a terminologia original será citada).

gistros digitais, também há uma diferença entre a preservação de registros digitais que são assinados ou selados digitalmente e aqueles que não são. Registros assinados ou selados digitalmente possuem um nível adicional de complexidade na forma de uma assinatura ou selo digital, o que torna sua preservação mais complicada.

Embora registros assinados digitalmente possam ser preservados por um período mais longo, eles podem perder sua validade legal se o registro digital não puder ser validado ou se perder sua propriedade de não-repúdio[9]. Se ocorrer um erro no processo de validação da assinatura digital, a confiabilidade do registro digital torna-se comprometida. Esse problema surge porque a revalidação de assinaturas digitais históricas geralmente não é suportada por softwares comum e requer preservação confiável a longo prazo de certificados digitais, CRLs (do inglês *Certificate Revocation Lists*, ou Listas de Certificados Revogados) etc. e, a longo prazo, outros elementos da infraestrutura histórica de PKI (do inglês *Public Key Infrastructure*, ou Infraestrutura de Chaves Públicas). Se algum dos elementos desse sistema apresentar mau funcionamento, a validação da assinatura digital falhará. Isso é especialmente importante ao preservar registros que contêm assinaturas digitais avançadas. (Herceg, Brzica, & Stančić, 2015)

### 4.2.1. Assinaturas digitais

Uma assinatura digital é um código criado de acordo com princípios criptográficos usando a Infraestrutura de Chaves Públicas conectada a um objeto digital, que serve como prova de que o objeto não foi adulterado e, em alguns casos, pode ser usado para autenticar a identidade do remetente. (Mihaljević, Mihaljević, & Stančić, 2015). A Lei de Assinatura Eletrônica, que esteve em vigor na Croácia até 7 de outubro de 2017, define assinatura digital como dados em formato eletrônico adicionados ou logicamente conectados a outros dados em formato eletrônico que servem para identificar o signatário e a confiabilidade do documento eletrônico assinado[10]. O Regulamento eIDAS da EU (do inglês *Electronic Identification, Authentication and Trust Services Regulation*, ou Regulamento de Identificação Eletrônica, Autenticação e Serviços de Confiança), que substituiu a Lei de Assinatura Eletrônica, define uma assinatura eletrônica como dados em formato eletrônico anexados ou logicamente associados a outros dados em formato eletrônico e que são usados pelo signatário para assinar.[11] Portanto, uma assinatura digital representa a tecnologia básica usada para verificar a autenticidade de um documento digital e um método de proteção do conteúdo do documento ou da comunicação eletrônica, enquanto o certificado digital, no qual ela se baseia, possibilita confirmar a identidade de uma pessoa física ou jurídica. Assim, o requisito básico para uma assinatura digital é a validação ou confirmação da originalidade ou autenticidade do signatário e do conteúdo da comunicação assinada. (Katulić, 2011)

Embora uma assinatura digital funcione com os mesmos princípios de uma assinatura tradicional, feita com tinta, existe uma diferença importante entre as duas. Ao assinar vários documentos em papel, geralmente se espera que a assinatura com tinta seja a mesma em todos os documentos.[12] Por outro lado, ao

---

9 Não-repúdio: No contexto digital, o não-repúdio é um serviço de segurança que garante que uma parte não possa negar a autoria de uma ação (como o envio de uma mensagem ou a realização de uma transação) ou o recebimento de uma informação. Ele fornece provas irrefutáveis da origem e/ou do destino dos dados, impedindo que o remetente ou o destinatário negue sua participação

10 Lei de Assinatura Eletrônica – NN 010/2002 (Parlamento Croata, 2002)

11 Regulamento eIDAS (Parlamento Europeu, 2014)

12 Em algumas legislações, não existe tal expectativa (por exemplo, nos EUA). E na Rússia, não há exigência oficial de unicidade da assinatura manuscrita – é mais uma prática comum do que uma exigência legal. Existem contextos em que diferentes assinaturas manuscritas são rotineiramente usadas pela mesma pessoa – por exemplo, funcionários de bancos utilizam assinaturas manuscritas simplificadas (às vezes completamente diferentes) para assinar documentos de transações.

assinar vários documentos digitais, a assinatura digital será uma *string* binária (sequência de bits) diferente, mas ainda estará associada ao documento e ao signatário. Em outras palavras, uma pessoa assina cada documento digital com uma assinatura digital diferente porque uma assinatura digital é enviada anexada a uma mensagem na forma de uma *string* binária. Se a mesma *string* fosse usada para vários documentos, qualquer pessoa que recebesse um documento assinado digitalmente poderia simplesmente copiar a *string* e anexá-la a outro documento, falsificando assim a assinatura de outra pessoa. Além das assinaturas eletrônicas básicas, que o Instituto Europeu de Normas de Telecomunicações (ETSI, do inglês *European Telecommunications Standards Institute*) define como essencialmente o equivalente a uma assinatura manuscrita, com dados em formato eletrônico anexados a outros dados eletrônicos como meio de autenticação, também existem assinaturas eletrônicas avançadas. De acordo com o Regulamento eIDAS, cuja definição é baseada na Diretiva 1999/93/CE, que já foi substituída, a assinatura eletrônica avançada deve atender aos seguintes requisitos: "a) estar vinculada exclusivamente ao signatário; b) ser capaz de identificar o signatário; c) é criada usando dados de criação de assinatura eletrônica que o signatário pode, com um alto nível de confiança, usar sob seu controle exclusivo; e d) ser vinculada aos dados assinados de tal forma que qualquer alteração subsequente nos dados seja detectável."[13]

### 4.2.2. Assinaturas digitais no contexto da criptografia

Para entender os princípios da segurança criptográfica em assinaturas digitais e certificados digitais, é importante observar o ambiente em que a assinatura digital surgiu e a infraestrutura e os métodos de segurança de documentos preexistentes que ela utilizava.

A palavra criptografia deriva da palavra grega κρύπτω ('kripto'), que significa oculto ou secreto, e γράφειν ('*grafein*'), que significa escrever. A criptografia lida com o estudo de métodos de envio de mensagens, nos quais a mensagem só pode ser lida pelo destinatário pretendido da mensagem. O objetivo da criptografia é, portanto, permitir que duas pessoas se comuniquem por meio de um canal de comunicação inseguro, de modo que uma terceira pessoa não possa entendê-las. A pessoa que envia a mensagem é chamada de remetente, a pessoa que recebe a mensagem é o destinatário e a terceira pessoa que tenta interceptar a mensagem é chamada de atacante. Usando uma chave acordada previamente, o remetente transforma a mensagem. A mensagem original é referida como texto simples, o procedimento de transformação como codificação ou criptografia. O resultado da criptografia é chamado de texto cifrado. O remetente envia o texto cifrado por meio de um canal de comunicação inseguro. Mesmo que o atacante intercepte a mensagem, ele não pode decifrá-la ou entendê-la sem conhecer a chave. A chave é, na verdade, uma função matemática que é usada para criptografia e descriptografia. Um criptosistema é, portanto, formado pela mensagem, o texto cifrado e a chave que contém as informações de criptografia e descriptografia. (Ibrahimpašić & Liđan, 2011)

Os criptosistemas podem ser: a) simétricos – aqueles que utilizam a mesma chave para criptografia e descriptografia (o que significa que remetente e destinatário devem trocar as chaves de forma segura); e b) assimétricos – aqueles que utilizam uma combinação de chave pública e chave privada (o que uma chave do par criptografa, somente a outra chave do mesmo par pode descriptografar, e vice-versa). Estes últimos, os criptosistemas assimétricos, formam a base para a Infraestrutura de Chaves Públicas (PKI) e sistemas de certificados digitais.

Os criptossistemas podem ser: a) simétricos — usam a mesma chave para criptografar e descriptografar (o que exige a troca segura da chave entre remetente e destinatário); e b) assimétricos — usam um par de chaves, pública e privada (o que é criptografado com uma só pode ser descriptografado com a outra, e vice-versa). Os criptossistemas assimétricos constituem a base da Infraestrutura de Chaves Públicas (PKI) e dos sistemas de certificados digitais.

---

13 Regulamento eIDAS (Parlamento Europeu, 2014)

Assinaturas digitais utilizam uma combinação de chaves públicas e privadas para que qualquer pessoa que visualize um documento assinado digitalmente possa verificar se a pessoa indicada na assinatura digital realmente assinou o documento. Esse processo é chamado de autenticação. Como as chaves servem como prova de autenticidade, em teoria, o signatário não pode negar que assinou o documento. Esse princípio é conhecido como irrevogabilidade ou não repúdio. (Ibrahimpašić & Liđan, 2011)

### 4.2.3. Confiança na identidade de uma pessoa que assina digitalmente um documento

O problema com o sistema de criptografia de chave pública é a questão da conexão segura entre a chave e a pessoa, ou seja, a questão da identidade da pessoa que assina digitalmente um documento permanece em aberto. A verificação bem-sucedida de uma assinatura não significa que o documento foi assinado pela pessoa indicada, mas apenas que foi assinado com a chave secreta que corresponde à chave pública. Portanto, no sistema de chave pública, há apenas confiança na troca bem-sucedida de chaves, mas a verdadeira identidade de uma pessoa não pode ser garantida. A solução para isso é o sistema PKI, ou seja, a infraestrutura de chaves públicas, onde uma terceira parte confiável (serviço de certificação) garante a identidade de uma pessoa e a conexão dessa pessoa com os pares de chaves privadas e públicas. Essa tecnologia é baseada nas recomendações ITU-T X.509 de 1988[14] e no RFC 3280 de 2002[15]. O valor de tal sistema está em sua flexibilidade para fornecer serviços e aplicações para identificação, autenticação, assinaturas digitais, bem como segurança e sigilo. O PKI é, na verdade, um sistema de certificados digitais, serviços de certificação e registro que verificam a identidade do usuário, sendo esse seu propósito principal.

O sistema PKI pode ser usado para possibilitar:

- verificação de identidade,
- integridade da informação,
- processos mais seguros de troca de dados,
- acesso público a serviços eletrônicos estatais e outros,
- aceitação de diversos documentos preenchidos eletronicamente, e
- comunicação segura com funcionários em locais remotos.

O sistema PKI fornece os componentes necessários para gerenciar (emitir, verificar e revogar) chaves públicas e certificados (bem como seu armazenamento e preservação). Ele também oferece autenticação segura dos participantes da comunicação, troca de documentos com possibilidade de criptografia, assinatura digital e assinatura conjunta, além de um registro único de chaves públicas na forma de um certificado digital.

O elemento básico deste sistema é o certificado digital. Ele é usado para implementações mais exigentes de criptografia de chave pública. Um certificado digital confirma a conexão entre uma chave privada pertencente a uma pessoa específica e a chave pública associada. Trata-se de um sistema em que a identidade da pessoa é armazenada junto com a chave pública correspondente, e toda a estrutura é assinada digitalmente por uma terceira parte confiável (serviço de certificação). Um certificado digital é emitido por um período limitado. Um certificado digital é emitido por um período limitado. A validade do certificado

---

14 Tecnologia da informação – Interconexão de Sistemas Abertos – O Diretório: Estruturas de certificados de chave pública e de atributos. A versão atual é a Edição 8, 10/2016, http://www.itu.int/itut/recommendations/rec.aspx?rec=X.509

15 Infraestrutura de Chave Pública da Internet X.509 (PKI): Perfil de Certificado e Lista de Revogação de Certificados (CRL). A versão atual é o RFC 5280, que foi atualizado pelo RFC 6818, https://tools.ietf.org/html/rfc5280

pode ser revogada, ou seja, o certificado pode ser cancelado mesmo antes do término do período para o qual foi originalmente emitido. A validade de um certificado digital pode ser verificada por meio da assinatura digital, mas deve haver uma confiança direta ou uma cadeia de confiança com a autoridade certificadora que o certifica. O formato do certificado digital é definido pela terceira versão do padrão X.509.

O próximo elemento é a Autoridade Certificadora (CA, do inglês *Certificate Authority*). Ela emite e revoga certificados digitais, gerencia-os, armazena-os e garante sua validade. Nesse sistema, a CA é uma entidade de confiança e uma terceira parte. A Autoridade de Registro (RA, do inglês *Registration Authority*) também pode participar do processo de emissão de certificados. Ela lida com as solicitações dos usuários para emissão de certificados digitais, registra os usuários e coopera com a CA durante a emissão dos certificados. A RA garante a identificação física correta dos usuários, assegurando assim a característica de não-repúdio das assinaturas digitais. Independentemente de a RA ser utilizada ou não, a CA é responsável pela emissão dos certificados digitais. Além da RA e da CA, existe um Repositório de Certificados (CR, do inglês *Certificate Repository*), onde são armazenadas as chaves públicas, os certificados dos usuários e as Listas de Revogação de Certificados (CRLs, do inglês *Certificate Revocation Lists*). Como já mencionado, os certificados digitais possuem um período de validade determinado (geralmente de dois a cinco anos) e podem ser encerrados ou revogados caso o usuário ou o certificado tenha sido comprometido. Existem duas formas de saber se um certificado digital foi revogado. A primeira é verificar se as informações de revogação do certificado foram publicadas na CRL. A segunda é utilizando o OCSP (do inglês, Online Certificate Status Protocol), um protocolo de internet usado para obter o status de revogação de um certificado[16].

### 4.2.4. Carimbos de Tempo Digitais

No contexto das assinaturas digitais, o carimbo de tempo digital desempenha um papel importante. Ele representa um certificado digitalmente assinado por uma entidade emissora de carimbos de tempo, que confirma a existência dos dados, documentos ou registros aos quais o carimbo de tempo se refere, no momento indicado no carimbo. O carimbo de tempo digital garante uma prova confiável de que os dados, documentos ou registros existiam anteriormente ou imediatamente antes do momento indicado no carimbo de tempo. Quaisquer alterações subsequentes nos dados, documentos, registros ou no carimbo de tempo não são permitidas e podem ser facilmente detectadas. Assim, o carimbo de tempo digital confirma: 1) que os dados, documentos ou registros em questão existiam naquela forma no momento indicado no carimbo de tempo; 2) que os dados, documentos ou registros não foram alterados após o momento indicado no carimbo de tempo. A Autoridade de Carimbo de Tempo (TSA, do inglês *Timestamping Authority*) assina digitalmente o valor *hash* dos dados, documentos ou registros junto com o valor do tempo (proveniente de uma fonte confiável, por exemplo, podendo estar vinculada ao Tempo Universal Coordenado, (UTC, do Inglês, *Coordinated Universal Time*), emitindo assim o carimbo de tempo digital, que é posteriormente combinado com os dados, documentos ou registros e a chave privada do signatário para criar a assinatura digital com a indicação do momento da assinatura.

## 4.3 Blockchain

Uma das possíveis soluções para a preservação a longo prazo de registros assinados digitalmente é a tecnologia blockchain. Blockchain é mais conhecida como a tecnologia por trás das moedas digitais (criptomoedas), que já está sendo aplicada em várias outras áreas para uma variedade de propósitos. Essa tecnologia é, por sua própria natureza, uma tecnologia de arquivamento, porque tudo o que está sendo registrado não pode mais ser alterado ou excluído.

---

16 Definido pelo RFC 2560 – X.509 Infraestrutura de Chave Pública da Internet Protocolo de Status de Certificado Online – OCSP de 1999. A versão atual é o RFC 6960 de 2013, https://tools.ietf.org/html/rfc6960

Blockchain representa um banco de dados distribuído de registros (transações) que armazena valores *hash* de dados, informações, transações, documentos ou outros registros. A tecnologia blockchain está associada ao conceito de Tecnologia de Registro Distribuído (DLT, do inglês *Distributed Ledger Technology*). O próprio termo é composto por duas partes: "bloco", que se refere ao conjunto completo de conteúdos, e "cadeia", que diz respeito à interconexão entre esses blocos. Essa cadeia cresce de forma linear, e a criação de um novo bloco, no contexto mais amplo das criptomoedas, é chamada de mineração[17].

### 4.3.1. Fundamentos da tecnologia blockchain e DLT

Para compreender melhor as tecnologias de blockchain e de DLT é necessário entender as tecnologias e conceitos subjacentes. Portanto, os próximos tópicos explicam os algoritmos de *hash*, a árvore de Merkle, o consenso distribuído e, por fim, o conceito de blockchain.

#### 4.3.1.1. Algoritmos de *hash*

*Hash*, ou resumo de mensagem (message digest), é uma função unidirecional que calcula uma sequência única de comprimento fixo a partir de qualquer dado, informação, documento ou registro de qualquer tamanho. A característica unidirecional significa que não é possível recriar o documento original a partir do conhecimento de seu *hash*. Durante um período de tempo definido, deve ser praticamente impossível criar "colisões", ou seja, ter dois ou mais registros significativos com o mesmo valor de *hash* (produzido por uma determinada função de *hash*). O valor de *hash* resultante também é chamado de impressão digital (digital *fingerprint*). Por isso, diz que o algoritmo de *hash* é resistente a colisões.

Outra característica do algoritmo de *hash* é que ele é pseudorrandômico. Isso significa que é imprevisível, mas também que, intencionalmente ou não, apenas um zero seja alterado para um em um fluxo binário, o *hash* resultante será significativamente diferente do original. Isso também implica que a função de *hash* é determinística, ou seja, sempre produzirá o mesmo *hash* a partir dos mesmos dados de entrada. (Drescher, 2017) É mais seguro do que a metodologia conhecida como Verificação de Redundância Cíclica (CRC do inglês *Cyclic Redundancy Check*[18]), pois é possível manipular os dados sem alterar o CRC previamente gerado ou, inversamente, alterar o CRC de qualquer arquivo para qualquer valor[19].

Existem muitas funções de *hash* diferentes[20], como Adler32, Haval, LM, MD, NTLM, RipeMD, SHA (Secure *Hash Algorithm*), Snefru, Tiger, Whirlpool, entre outras. Algumas delas podem ter diferentes níveis de força, ou seja, diferentes comprimentos de sequência, como MD2, MD4, MD5 ou SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, etc.[21] A Figura 1 mostra os diferentes valores de *hash* do texto simples do título desta pesquisa.

---

17 [N. do T.] Mineração (Mining): No contexto de blockchain e criptomoedas, "mineração" refere-se ao processo computacional de validação de transações e criação de novos blocos de dados que são adicionados à cadeia.

18 [N. do T]. CRC (*Cyclic Redundancy Check*) é um método de verificação de integridade de dados amplamente utilizado para detectar erros acidentais em transmissões ou armazenamento de informações. Diferente de um algoritmo de hash criptográfico, o CRC não é projetado para fins de segurança, pois não oferece resistência a manipulações intencionais dos dados. Sua principal função é garantir que os dados não foram corrompidos por falhas de hardware ou ruído na comunicação.

19 Forçar o CRC de um arquivo para qualquer valor (Nayuki, 2016).

20 [N. do T].: Funções de hash são algoritmos que transformam dados de qualquer tamanho em uma sequência única de comprimento fixo, chamada valor de hash ou impressão digital. Elas são amplamente utilizadas para garantir a integridade e a autenticidade de informações em diversas aplicações de segurança da informação.

21 Algumas das funções de hash mencionadas estão desatualizadas há muito tempo e são incluídas aqui por razões históricas e de demonstração.

| | |
|---|---|
| Original text | Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) |
| Original bytes | 4d6f64656c20666f722050726573657276174696f6e206f66... (length=137) |
| Adler32 | ae4831e2 |
| CRC32 | ed29d1fa |
| Haval | 15a4971d923ad4a7adce708c83fbb512 |
| MD2 | f16faa8a18b6695714cfc34ea3277c51 |
| MD4 | d51acfc5b54f21f225fe82819ddcfc21 |
| MD5 | 9b3a1431647b127f5d133f0c54adb0f5 |
| RipeMD128 | ad9f290a21c91df7a9d5460bf800fc0a |
| RipeMD160 | 069b84458115557d3025b308d3663925979cf36d |
| SHA-1 | 2f8a2914921342addb47ed18b89e0b2104a113c0 |
| SHA-256 | 064bfb90c5e6587bbd8a55122f8a53daaaa79da1b5b9ef6108072f4bdf83ab65 |
| SHA-384 | 3aca9c561d4be7db34c651377699ac40e1521be9c8b0eebb92e2e2a51f0bcae589563a1b34f4a00dba3c68bd0005fb94 |
| SHA-512 | 8380e7138bbadf22372b9326742bf9c3fee10f1a1b2d9b133abfc45292a976bdb1bcb7fbede132c87aaab90b5bdd4a08cf5c97d960c16499d8b7eef99771ee15 |
| Tiger | ca2d84335f6ee13101f69dcccad0cbe79a6621d45580f5db |
| Whirlpool | c8cad58472c1c913b1b15ae1d58bb61749776daa4c75842ac2bff15e7d8312e83b34535e85f01e1275eed4751bdd96f4351c5e87344852792aeefabd6300ef7e |

Figura 1. Exemplo de valores de *hash*

| | |
|---|---|
| Original text | Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) |
| SHA-256 | 064bfb90c5e6587bbd8a55122f8a53daaaa79da1b5b9ef6108072f4bdf83ab65 |
| Original text | Model for Preservation of Trustworthiness of the Digitally Signed; Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) |
| SHA-256 | ec6ab344f1f433b6f680ef71a3bef0053deff852e57abb7725158889e7b2d791 |

Figura 2. Exemplo da característica pseudoaleatória de uma função de *hash*.

A Figura 2 mostra dois valores de *hash* significativamente diferentes resultantes da aplicação do mesmo algoritmo de *hash* SHA-256 para duas entradas de texto simples que diferem apenas por um único caractere – um ponto e vírgula é usado em vez de uma vírgula.

#### 4.3.1.2. Árvore de Merkle

Os valores de *hash* podem ser combinados em um único *hash*. Isso será ilustrado pelo seguinte exemplo (veja a Figura 3).

Uma pequena empresa cria 10 documentos pela manhã e 10 documentos à tarde. Um valor de *hash* é calculado para cada documento. Ao meio-dia, todos os 10 valores de *hash* da manhã são combinados em um único *hash*, chamado de "*hash* da manhã". No final do dia, por exemplo, na segunda-feira, todos os 10 valores de *hash* da tarde são novamente combinados em um único "*hash* da tarde". Em seguida, os valores de *hash* da manhã e da tarde são combinados para gerar um único valor de *hash* para a segunda-feira. Esse *hash* é chamado de root *hash* (*hash* raiz) ou top *hash* (*hash* superior).

Este exemplo é expandido nas Figuras 5 a 9, que explicam o conceito de blockchain.

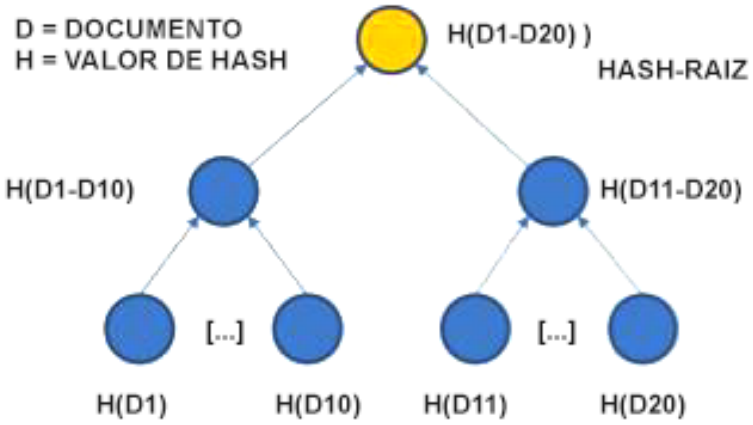


Figura 3. Árvore de Merkle

Essa abordagem foi introduzida pela primeira vez em 1980 por Ralph C. Merkle. (Merkle, 1980) Como a estrutura se assemelha a uma estrutura de árvore (invertida), foi nomeada de árvore de Merkle. Antes de explicar o conceito de blockchain, que utiliza a abordagem da árvore de Merkle, será explicado o conceito de consenso distribuído.

#### 4.3.1.3. Consenso distribuído

A tecnologia blockchain utiliza uma rede distribuída (*peer-to-peer*). Basicamente, existem três tipos de topologias de rede: centralizada, descentralizada e distribuída[22] (Figura 4).

A rede centralizada possui um servidor central ao qual outros computadores estão conectados. Esse tipo de topologia de rede tem controle centralizado e um único ponto de falha (o servidor central). Hackers podem direcionar ataques ao servidor central.

A rede descentralizada possui vários servidores aos quais outros computadores estão conectados. Esse tipo de topologia de rede tem controle descentralizado e é mais segura do que a rede centralizada, mas os servidores ainda podem ser identificados e atacados.

A rede distribuída não possui centro(s), pois todos os computadores interconectados são tratados de forma igual. Esse tipo de topologia de rede não possui um único ponto de controle e, portanto, não possui um único ponto de ataque.

Os dois primeiros tipos de topologia de rede também podem ser vistos como aplicados à estrutura de governos, instituições ou organizações. Existem escritórios centrais, filiais, etc. Isso também significa que o poder é mais ou menos centralizado, ou que é necessário um terceiro confiável na comunicação ou troca. Por exemplo, se uma pessoa A deseja enviar uma certa quantia de dinheiro para uma pessoa B, pelo menos a pessoa B precisa ter uma conta bancária. O banco, nesse exemplo, é o terceiro confiável. Por outro lado, com a aplicação do conceito de rede distribuída, pode-se evitar a necessidade de um terceiro confiável e realizar a troca de dinheiro diretamente.

Isso é possível aplicando o princípio do consenso distribuído, no qual cada participante (nó) verifica cada evento no livro-razão ("livro principal"/banco de dados). O consenso é usado para determinar a verdade, ou seja, para evitar o gasto duplo da mesma quantia de dinheiro ou duas instâncias diferentes do mesmo registro. O evento (por exemplo, uma transação monetária ou o registro de um dado) é válido apenas se a maioria qualificada (50%+1 nó) concordar com ele.

---

22 Os grupos da ISO reconheceram a diferença entre a arquitetura física e a arquitetura de controle/governança. Um sistema centralizado pode ter redundância e elementos distribuídos, por exemplo, pode haver várias cópias do servidor de controle principal situadas em diferentes locais geográficos.


Figura 4. Três tipos de topologia de rede23

#### 4.3.1.4. Conceito de Blockchain

A abordagem da árvore de Merkle foi utilizada por Satoshi Nakamoto para criar a moeda virtual/cripto-moeda Bitcoin (Nakamoto, 2008), o que, por sua vez, impulsionou a aplicação mais ampla da tecnologia blockchain.

A tecnologia blockchain cria uma cadeia de blocos interligados. Isso será ilustrado estendendo o exemplo que explica a árvore de Merkle, mostrado na Figura 3. A empresa mencionada anteriormente pode repetir o processo de hashing de segunda-feira na terça-feira. Isso resultará em dois valores de *hash* – um para cada dia. Esses dois valores podem ser posteriormente combinados em um único *hash* superior, unindo os *hashes* individuais de segunda e terça-feira. Esse único valor de *hash* seria então combinado com o valor de *hash* de quarta-feira para criar um novo *hash* superior, e assim por diante. Cada novo *hash* superior é calculado a partir do *hash* do dia e do *hash* superior anterior, vinculando assim os *hashes* superiores (Figura 5).

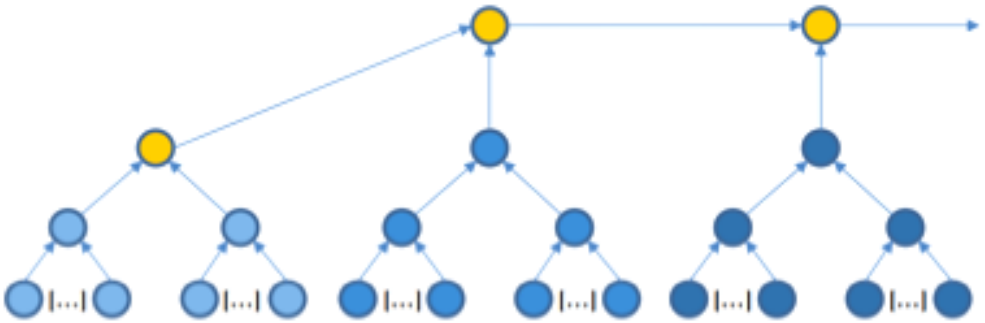

Figura 5. Vinculação dos valores de *hash*

O conceito de blockchain se baseia nisso e solicita que todos os nós participantes confirmem a criação do novo *hash* superior. De acordo com o princípio do consenso distribuído, um novo bloco é confirmado quando a maioria qualificada concorda com ele (Figura 6).

As criptomoedas também implementam tarefas computacionais demoradas chamadas de "quebra-cabeças de *hash*" para calcular o *hash* do novo bloco, ou seja, para implementar o conceito de prova de trabalho (*proof of work*) e, consequentemente, criar o valor da criptomoeda, que se origina dos recursos computacionais e do tempo utilizado. No entanto, a explicação desse processo está fora do escopo deste relatório.

---

23 Image source: http://bluenetworks.weebly.com/syngeneia-in-the-history-of-pergamon.html

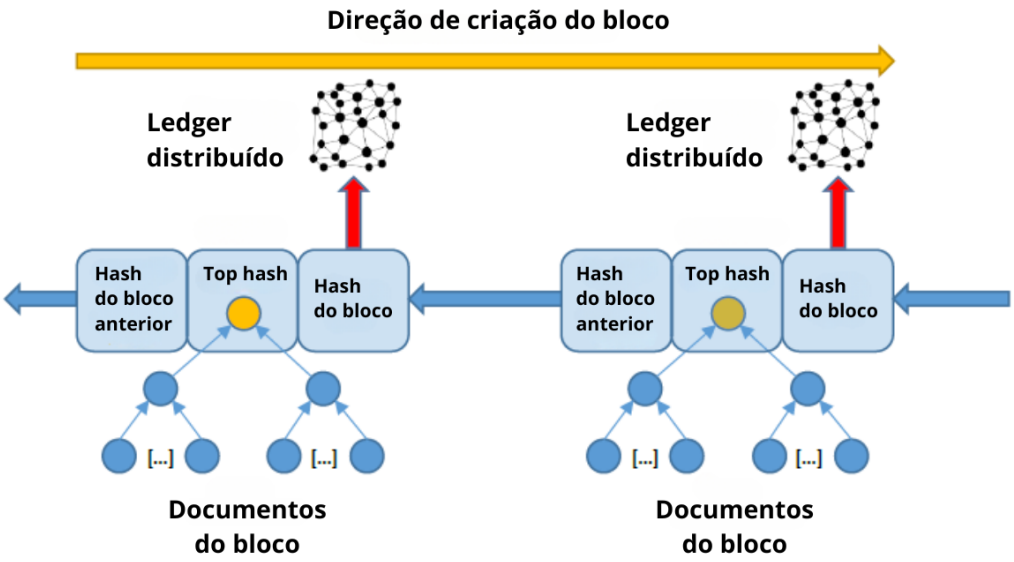


Figura 6. Criação de blockchain

Também é importante destacar que um bloco pode conter muitos *hashes* (eventos, transações) que são agrupados em um único bloco (Figura 7). Novos blocos, quando confirmados, recebem um carimbo de data e hora e são registrados por todos os nós participantes, criando assim o livro-razão distribuído.

Novos blocos são criados em intervalos regulares de tempo. Dependendo da criticidade temporal para a criação de novos blocos, os intervalos de tempo podem variar, por exemplo, de 10 ou 15 minutos para cada bloco, a um minuto ou, quando a latência é importante, podem ser reduzidos para um intervalo de apenas um segundo.

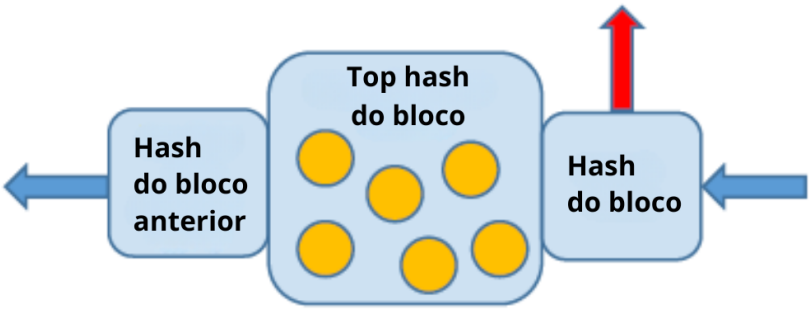


Figura 7. Múltiplos *hashes* combinados em um único bloco

A blockchain possui várias vantagens. Primeiramente, embora seja possível armazenar dados na blockchain, neste exemplo, apenas os *hashes* são armazenados (registrados). Os dados reais, documentos ou registros que são transformados em *hashes* são armazenados no sistema institucional e permanecem sob controle.

Em segundo lugar, cada bloco adicional reforça os blocos anteriores, já que a cadeia é formada por blocos interligados. Em terceiro lugar, qualquer tentativa de modificar um bloco invalidaria todos os blocos subsequentes e seria facilmente detectada (Figura 8). Portanto, não é possível realizar alterações nos blocos já criados.

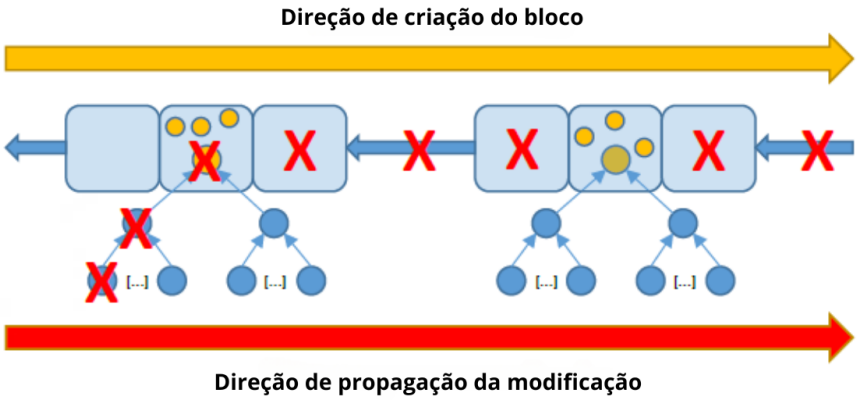


Figura 8. Propagação da modificação de *hash* através da blockchain

A blockchain contém a prova de que um *hash*, e nesse sentido que um dado, documento, registro ou transação, fazia parte do conjunto original de *hashes* sobre o qual a cadeia foi construída (Figura 9).

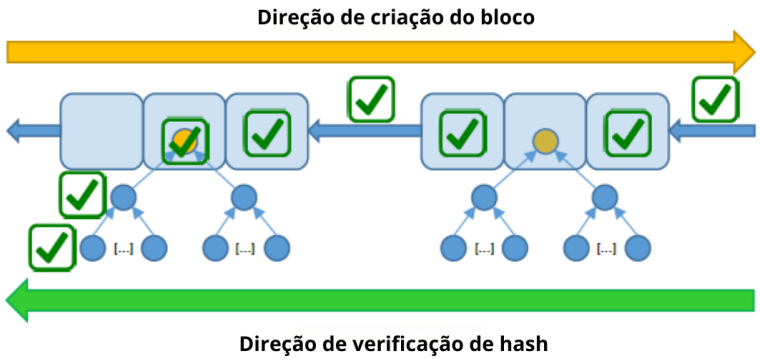


Figura 9. Verificação de um valor de *hash* na blockchain

Deve-se notar que, ao obter controle sobre a maioria qualificada dos nós interconectados, um atacante pode passar a controlar a criação de novos blocos. No entanto, para alterar um valor de *hash* que já foi registrado na blockchain, o atacante precisaria recalcular todos os *hashes* dos blocos subsequentes. Isso pode ser uma limitação caso a blockchain seja utilizada sem o proof of work (prova de trabalho); por outro lado, se o *proof of work* for utilizado, os custos computacionais e de tempo superam os possíveis benefícios. Ainda assim, o modelo *TrustChain* desenvolvido neste estudo abordou o problema do uso da blockchain sem o *proof of work* (ver Capítulo 7.2).

O problema do enfraquecimento dos algoritmos criptográficos usados para criar os valores de *hash* originais ao longo do tempo pode ser resolvido ao aplicar um algoritmo de *hash* mais forte no próximo bloco e continuar a usá-lo. Outra solução seria alcançar um consenso da maioria qualificada dos nós para cortar a cadeia no ponto em que os algoritmos mais fortes devem ser usados, iniciando assim uma nova cadeia. A parte antiga da cadeia deve ser preservada com segurança por todos os nós da rede e pode ser envolvida com um *hash* de um algoritmo mais forte por razões de segurança.

Para qualquer blockchain distribuída, é fundamental atingir um tamanho crítico, ou seja, envolver um número significativo de nós para garantir segurança contra possíveis ataques. O que constitui um número significativo depende do propósito da implementação da blockchain e da atratividade para possíveis atacantes. Nesse contexto, deve-se mencionar que existem dois tipos possíveis de implementação de blockchain – uma blockchain pública e uma blockchain privada. A Tabela 1 resume as diferenças entre as duas.

Tabela 1. As diferenças entre blockchain pública e privada

| Blockchain pública | Blockchain privada |
|---|---|
| Qualquer pessoa pode registrar (gravar) dados livremente, sem necessidade de autorização de qualquer autoridade | Apenas participantes conhecidos e confiáveis (autorizados por uma autoridade) podem registrar (gravar) dados livremente |
| Sem ponto único de controle | Sem ponto único de controle (exceto fase de autorização inicial) |
| Anonimato (relativo) | Sem anonimato |
| Exemplo: Bitcoin, Ethereum | Exemplo: um grupo de Arquivos parceiros |

O que falta, do ponto de vista arquivístico até agora, é o vínculo arquivístico. Lemieux e Sporny observam que "mesmo que a natureza ordenada no tempo dos registros transacionais seja preservada, o vínculo com seu contexto procedimental e a relação com outros registros transacionais relacionados ao mesmo procedimento não é." Eles propõem que "por meio do uso de ontologias para representar o contexto procedimental das entradas no livro-razão, é possível instanciar o vínculo arquivístico entre as entradas do livro-razão como registros de uma variedade de transações. " (Lemieux & Sporny, 2017)

Levando em consideração todas as características da blockchain, bem como suas tecnologias e conceitos subjacentes, pode-se concluir que a blockchain pode ser usada para:

- confirmar a integridade de um registro,
- confirmar que um registro existia ou foi criado em um determinado momento (ou seja, não após ter sido carimbado com data e registrado na blockchain),
- confirmar a sequência de registros,
- apoiar/reforçar a não-repudiação de um registro,
- melhorar as possibilidades de validação de registros assinados digitalmente durante a preservação de longo prazo, e
- garantir que processos digitais não possam ser manipulados (ver Capítulo 7.2).

### 4.3.2. Aplicações da tecnologia blockchain

"A tecnologia blockchain atraiu atenção como base para criptomoedas, como o Bitcoin, mas suas capacidades vão muito além disso, permitindo que aplicações tecnológicas existentes sejam amplamente melhoradas e que novas aplicações, antes impraticáveis, sejam implementadas. Também conhecida como tecnologia de livro-razão distribuído (*distributed ledger technology*), a blockchain é esperada para revolucionar a indústria e o comércio, impulsionando mudanças econômicas em escala global, pois é imutável, transparente e redefine a confiança, permitindo soluções seguras, rápidas, confiáveis e transparentes, que podem ser públicas ou privadas. Ela pode empoderar pessoas em países em desenvolvimento com identidade reconhecida, propriedade de ativos e inclusão financeira. " (Underwood, 2016)

Existem muitas aplicações da blockchain que podem transformar a sociedade – algumas delas incluem serviços financeiros baseados em blockchain, aplicações de propriedade inteligente (por exemplo, registro de títulos de propriedade), contratos inteligentes, aplicações nos setores de saúde ou música, notarização, rastreamento de procedência, bem como aplicações de governo eletrônico, como votação pública, gestão de identidade, etc. Além disso, a aplicação da blockchain na votação pública e no setor de saúde será explorada a seguir.

#### 4.3.2.1. Blockchain e DLT em sistemas de votação pública

Após o enorme sucesso do Bitcoin e de outras tecnologias relacionadas à blockchain, bem como seu impacto em muitos setores além do financeiro, surge a questão de saber se a mesma tecnologia blockchain pode ser aplicada para ajudar os processos democráticos modernos, que ainda dependem principalmente de papel (Bradbury, 2014).

"A blockchain pode servir como meio para registrar, rastrear e contar votos, de modo que nunca haja dúvidas sobre fraude eleitoral, registros perdidos ou manipulação. Ao registrar votos como transações dentro da blockchain, os eleitores podem concordar com a contagem final porque podem contar os votos por si mesmos e, devido ao rastro de auditoria da blockchain, podem verificar que nenhum voto foi alterado ou removido, e que nenhum voto ilegítimo foi adicionado. " (Huminski, 2017)

O Parlamento Europeu (Boucher, 2016) destaca que, desde o início do século, o voto eletrônico tem sido considerado um desenvolvimento promissor e (eventualmente) inevitável, que poderia acelerar, simplificar e reduzir os custos das eleições. Agora, podemos continuar confiando em autoridades centrais para gerenciar eleições ou usar a tecnologia blockchain para distribuir um registro aberto de votação entre os cidadãos. Muitos especialistas concordam que o voto eletrônico exigiria desenvolvimentos revolucionários em sistemas de segurança. O debate gira em torno de saber se a blockchain representará um desenvolvimento transformador ou apenas incremental, e quais seriam suas implicações para o futuro da democracia. Swan (Swan, 2015) argumenta que é possível aplicar a ideia de usar a tecnologia blockchain para fornecer serviços tradicionalmente oferecidos pelo Estado de maneira descentralizada, mais barata, eficiente e personalizada.

Embora ainda não exista uma discussão abrangente em nível acadêmico sobre possíveis modelos de governança baseados em blockchain, alguns autores (Atzori, 2016) propuseram possíveis aplicações da tecnologia blockchain no setor governamental. Com base em Swan (Swan, 2015), Atzori (Atzori, 2016), entre outros, que resumem os principais princípios e problemas de governança que a blockchain poderia mitigar:

Ao longo da história, organizações políticas centralizadas, como o Estado, a burocracia e a democracia representativa, têm sido uma solução para o problema de escalabilidade. Uma autoridade central em qualquer organização hierárquica pode ser definida, em termos computacionais, como um Single Point of Failure (SPOF, ou Ponto Único de Falha): se seu funcionamento não for ideal, todo o sistema e seus participantes serão negativamente afetados. A autoridade vertical centralizada tornou-se o principal modelo organizacional na sociedade, simplesmente porque, até agora, não havia uma alternativa melhor. Pela primeira vez na história, os cidadãos podem alcançar consenso e coordenação em nível global por meio de procedimentos ponto a ponto (*peer-to-peer*) verificados criptograficamente, sem a intermediação de terceiros. A tecnologia blockchain pode levar a uma nova era de descentralização em larga escala, na qual o fator humano é minimizado. Nesse cenário, o software de governo descentralizado poderia ser usado como uma plataforma colaborativa para governança *faça você mesmo* (*DIY governance*), permitindo que qualquer pessoa crie seus próprios serviços governamentais (em uma "nação blockchain"). Assim, muitos novos modelos e serviços de governança descentralizada podem ser implementados e experimentados por meio da blockchain (Swan, 2015).

**Poder dos indivíduos**

Enquanto o Estado baseia sua ação na coerção, a blockchain pode fornecer serviços de governança de maneira mais eficiente e descentralizada, sem depender do uso da força. Isso permite uma difusão de autoridade mais horizontal e distribuída, na qual a fonte de legitimidade são os próprios indivíduos. Usando a blockchain como um repositório público permanente e seguro por criptografia, agentes humanos, como representantes, podem ser substituídos por contratos inteligentes (*smart contracts*) e Corporações Autônomas Descentralizadas (*Decentralized Autonomous Corporations - DACs*) (Swan, 2015).

A tecnologia blockchain permite serviços governamentais mais granulares e personalizados. Utilizando a blockchain como um repositório público permanente de registros, é possível armazenar todos os documentos legais do governo, como contratos, carteiras de identidade, passaportes, escrituras de terras, etc., de forma mais barata, eficiente e descentralizada. Qualquer pessoa pode criar uma blockchain privada e um sistema de governança descentralizado *faça você mesmo* (Swan, 2015).

Para implementar esses dois princípios com tecnologias baseadas em blockchain, uma das áreas-chave é o desenvolvimento de sistemas que tornem a democracia mais eficaz e, ao mesmo tempo, mais transparente. Para alcançar esse objetivo, há a necessidade de sistemas de votação descentralizados.

O protocolo blockchain é um meio de registrar e verificar registros de forma transparente e distribuída entre os usuários. Normalmente, os votos são registrados, gerenciados, contados e verificados por uma autoridade central. A votação eletrônica habilitada por blockchain (*Blockchain-Enabled Voting* - BEV) permitiria que os eleitores realizassem essas tarefas por conta própria, mantendo uma cópia do registro de votação. O registro histórico não poderia ser alterado, pois outros eleitores perceberiam que o registro difere do deles. Votos ilegítimos seriam muito mais difíceis de adicionar, pois outros eleitores poderiam verificar se os votos eram compatíveis com as regras (talvez porque já tenham sido contados ou não estejam associados a um registro de eleitor válido). A BEV transferiria poder e confiança dos atores centrais, como autoridades eleitorais, para fomentar o desenvolvimento de um consenso comunitário habilitado por tecnologia (Boucher, 2016).

**Três abordagens possíveis para sistemas de votação baseados em blockchain**

Swan (2015) apresenta uma visão geral de três abordagens possíveis para criar tais sistemas:

1. **Sistema de Democracia Líquida** - No sistema de Democracia Líquida, um membro de um partido pode atribuir um voto por procuração a qualquer outro membro, designando assim um delegado pessoal em vez de votar em um representante. A ideia de tomada de decisão delegada, apoiada e executada em estruturas baseadas em blockchain, pode ter ampla aplicabilidade além do contexto de votação política e formulação de políticas. Ideias para uma aplicação mais granular da democracia têm sido propostas há anos, mas somente agora, com a Internet e o advento de sistemas como a tecnologia blockchain, esses tipos de mecanismos complexos e dinâmicos de tomada de decisão se tornam viáveis para implementação em contextos do mundo real.
2. **Eleições por Amostra Aleatória** - Além da democracia delegativa, outra ideia que poderia ser implementada com governança baseada em blockchain são as eleições por amostra aleatória. Nessas eleições, eleitores selecionados aleatoriamente recebem uma cédula pelo correio e são direcionados a um site de votação que apresenta debates entre candidatos e declarações de ativistas. Conforme articulado pelo criptógrafo David Chaum, a ideia é que (como no ideal de uma pesquisa) eleitores selecionados aleatoriamente seriam mais representativos (ou poderiam, pelo menos, incluir eleitores sub-representados) e teriam mais tempo para deliberar sobre questões em casa, buscando seus próprios recursos de tomada de decisão em vez de serem influenciados por publicidade. A tecnologia blockchain poderia ser um meio de implementar eleições por amostra aleatória de maneira confiável, em larga escala e pseudônima.
3. **Futarquia: Democracia em Dois Passos com Votação** - Outro conceito é a futarquia[24], um processo em dois níveis no qual os indivíduos primeiro votam em resultados gerais especificados (como "aumentar o PIB") e, em seguida, votam em propostas específicas para alcançar esses resultados. O primeiro passo seria realizado por meio de processos de votação regulares, e o segundo passo por meio de mercados de previsão. Assim como nas eleições por amostra aleatória, a tecnologia blockchain poderia implementar o conceito de futarquia de maneira mais eficiente, em larga escala (descentralizada, confiável, registrada e pseudônima). Há a possibilidade de que modelos de votação

24 O nome "futarquia" vem do governo por mercados futuros. (Hanson, 2000)

e especificação de preferências (como a estrutura de votação em dois níveis da futarquia usando tecnologia blockchain) se tornem uma norma comum e amplamente difundida para todos os processos complexos de tomada de decisão multipartidária.

Embora tenham ocorrido desenvolvimentos significativos sobre como a blockchain poderia ser implementada no setor governamental, ainda há muito debate. Sistemas propostos, como o BitCongress (Rockwell), combinam conceitos democráticos tradicionais, tecnologia blockchain e Bitcoin como base subjacente. A principal questão aqui é garantir a integridade do voto de ponta a ponta – onde a blockchain pode ser um meio útil para garantir a integridade do voto no *back-end*. A questão-chave é como garantir confiança generalizada na segurança e legitimidade do sistema. Assim como nas eleições baseadas em papel, não basta que o resultado seja justo e válido. Todo o eleitorado, mesmo que esteja desapontado com o resultado, deve aceitar que o processo foi legítimo e confiável. Portanto, além de fornecer segurança e precisão reais, a BEV também deve inspirar ampla confiança e confiança pública. Como o protocolo blockchain é bastante complexo, isso pode ser uma barreira para a aceitação pública generalizada da BEV (Boucher, 2016).

#### 4.3.2.2. Blockchain e DLT no setor de saúde

"As instituições de saúde sofrem com a incapacidade de compartilhar dados com segurança entre plataformas. Uma melhor colaboração de dados entre os prestadores de serviços significa maior probabilidade de diagnósticos precisos, maior probabilidade de tratamentos eficazes e maior capacidade dos sistemas de saúde de fornecer cuidados econômicos. A Blockchain pode permitir que hospitais, pagadores e outras partes na cadeia de valor da saúde compartilhem o acesso às suas redes sem comprometer a segurança e a integridade dos dados. (...) A Blockchain permitiria que o hospital vinculasse os pacientes aos seus dados, em vez de vinculá-los à sua identidade. " (Huminski, 2017)

As tecnologias e dispositivos da Internet estão se tornando mais relevantes em todos os aspectos da vida humana, incluindo a saúde. Os dispositivos podem ser aplicados para ajudar a diagnosticar doenças e salvar vidas humanas. Além disso, espera-se que os registros de saúde cresçam exponencialmente nos próximos anos, à medida que mais dados são coletados diariamente. O crescimento dos dados será liderado pelo desenvolvimento de novos métodos de diagnóstico e dispositivos de análise. Portanto, é necessário analisar quais tecnologias são adequadas para uso em um futuro próximo, a fim de garantir conexões seguras e armazenamento de dados. Para usar todos os benefícios do avanço tecnológico na área da saúde, grandes bancos de dados são criados e aplicativos desenvolvidos que podem usar dados para pesquisa, comparação e análise preditiva, terapia, diagnóstico ou previsão de doenças na área da saúde. O plano nacional da Casa Branca para o futuro da Inteligência Artificial (IA) no domínio da saúde e suas recomendações para ações específicas por agências federais e outros atores determinam os regulamentos de saúde no domínio da segurança pública. Suas recomendações estão amplamente relacionadas à administração de big data e privacidade. (Casa Branca – Conselho Nacional de Ciência e Tecnologia, 2016)

No contexto desta tecnologia, surgem inúmeros problemas potenciais, por exemplo, o que aconteceria se um indivíduo mal-intencionado alterasse o prontuário médico de alguém, afirmando que a pessoa não é alérgica à penicilina quando, na verdade, ela é. Durante o próximo tratamento hospitalar, o paciente poderia receber penicilina e morrer devido à violação de dados. Outro exemplo seria controlar um marca-passo ou mesmo um injetor de insulina que está conectado ao médico ou hospital de referência para enviar parâmetros. Se esses dados pudessem ser interceptados e manipulados, os pacientes poderiam ser induzidos a um derrame, ter seu marca-passo desligado ou receber uma dose maior de insulina.

Quando se trata de tecnologias utilizadas na área da saúde, existem diferentes produtos e dispositivos no mercado. Um dispositivo interessante é um implante cerebral que pode ajudar a restaurar partes danificadas do cérebro ou aumentar as capacidades de memória (Drummond, 2010). Dispositivos que podem ser conectados a *smartphones* para enviar dados médicos usando a internet ou dados móveis estão no

mercado há vários anos e seu número está crescendo diariamente. Além disso, o mercado e as funções dos smartwatches estão crescendo, assim como seu uso potencial no monitoramento de saúde e coleta de dados. Dispositivos que medem pulso, pressão arterial, alterações na pele, ECG, EEG e até mesmo dispositivos móveis de teste de DNA para *smartphones* estão disponíveis no mercado atualmente.

Um dos tópicos importantes é a segurança na comunicação entre novos dispositivos médicos e bancos de dados médicos. Até o momento, essa comunicação não é segura o suficiente para garantir a segurança dos pacientes. Para permitir que as tecnologias existentes sejam usadas em tarefas de saúde básicas e vitais, é necessária mais pesquisa no campo da comunicação altamente segura. Como o tópico trata essencialmente da segurança da informação, os melhores métodos disponíveis para este tipo de diagnóstico indireto vêm do setor financeiro.

No entanto, para que esta tecnologia seja implementada com sucesso, proteger as conexões e a segurança dos registros é crucial. Para combater este problema, o governo dos EUA patrocinou um concurso em 2016 cujo objetivo era encontrar a melhor solução para usar a tecnologia blockchain na área da saúde. Uma solução, desenvolvida como parte do concurso, foi a ideia de usar dados móveis para monitorar o estado de saúde de uma pessoa, enviando dados por meio de um aplicativo especial para seu médico de referência, enquanto outra solução tratava da segurança de dados de bancos de dados e registros. A Estônia, como líder em governo eletrônico na UE, anunciou em 2016 sua parceria com a empresa startup Guardtime, a fim de proteger mais de 1 milhão de registros de saúde de pacientes usando um sistema blockchain. Sua parceria com a empresa startup blockchain demonstra que as tecnologias emergentes, como a blockchain neste exemplo, podem ser usadas para proteger registros de saúde confidenciais. Os requisitos de protocolo de saúde existentes, como o *Health Information Exchange* (HIE) e o *Integrating the Healthcare Enterprise* (IHE), podem ser atendidos usando a tecnologia blockchain como uma nova forma de padronização de dados para distribuição de dados de saúde. Organizações de saúde e governamentais gastam muito tempo e dinheiro na configuração e gerenciamento de sistemas de informação e trocas de dados. A tecnologia de código aberto, as propriedades e a natureza distribuída da blockchain podem ajudar a reduzir o custo dessas operações. Os registros eletrônicos de saúde baseados em blockchain podem permitir o compartilhamento e o acesso aos dados, ao mesmo tempo em que os protegem completamente.

## 4.4 Normas relevantes e marcos legais

A preservação de longo prazo de registros assinados digitalmente exige que eles mantenham suas características básicas – autenticidade, confiabilidade, integridade e usabilidade. Para alcançar esse objetivo, é necessário basear-se em normas relevantes e, geralmente, em um marco legal nacional.

### 4.4.1. ISO 15489 – Informação e documentação – Gestão de registros

Em 2001, a Organização Internacional de Normalização (ISO) publicou dois documentos que, juntos, formam duas partes de uma nova norma internacional de gestão de registros – ISO 15489 – Informação e documentação – Gestão de registros. A primeira parte refere-se à norma de forma geral, enquanto a segunda fornece diretrizes técnicas anteriormente conhecidas como um relatório técnico.

Com a aplicação da norma ISO 15489-1:2016 – Informação e documentação – Gestão de registros, parte um – Conceitos e Princípios, a norma ISO 15489-1:2001 foi considerada obsoleta.

De acordo com a ISO 15489, os registros eletrônicos devem manter sua autenticidade, o que significa que, após a conclusão de qualquer procedimento de preservação digital, eles ainda devem ser autênticos, completos e utilizáveis, além de manter o conteúdo, a estrutura e o contexto em relação a outros registros preservados[25].

25 **ISO 15489-1:2016** (Organização Internacional de Normalização, 2016)

### 4.4.2. ISO 14721 – Modelo de Referência do Sistema Aberto de Informação Arquivística

O Modelo de Referência do Sistema Aberto de Informação Arquivística (OAIS, do inglês *Open Archival Information System* - Sistema de Informação Arquivística Aberta) é uma das possíveis soluções técnicas para a preservação de longo prazo. O modelo foi desenvolvido pelo Comitê Consultivo para Sistemas de Dados Espaciais (CCSDS) em parceria com a NASA, em 1999. Tornou-se um padrão ISO em março de 2003 (ISO 14721:2003). A versão mais recente é de 2012 (ISO 14721:2012)[26] e está atualmente em revisão.

O modelo de referência OAIS é aplicável a qualquer arquivo digital, mas deve ser expandido e adaptado de acordo com os requisitos específicos dos criadores de documentos e dos arquivos digitais. O modelo OAIS refere-se à preservação digital de longo prazo de registros como objetos e pacotes de informação (SIP, AIP, DIP). Ele define um modelo de informação e um modelo funcional de um arquivo digital.

**ISO 14721:2012:**

- Fornece uma estrutura para a compreensão e maior conscientização sobre os conceitos arquivísticos necessários para a preservação e o acesso de longo prazo à informação digital;
- Oferece os conceitos necessários para que organizações não arquivísticas sejam participantes eficazes no processo de preservação;
- Fornece uma estrutura, incluindo terminologia e conceitos, para descrever e comparar arquiteturas e operações de arquivos existentes e futuros;
- Oferece uma base para descrever e comparar diferentes estratégias e técnicas de preservação de longo prazo;
- Fornece uma base para comparar os modelos de dados de informações digitais preservadas por arquivos e para discutir como os modelos de dados e as informações subjacentes podem mudar ao longo do tempo;
- Oferece uma estrutura que pode ser expandida por outros esforços para cobrir a preservação de longo prazo de informações que não estão em formato digital (por exemplo, mídias físicas e amostras físicas);
- Expande o consenso sobre os elementos e processos para a preservação e o acesso de longo prazo à informação digital, promovendo um mercado maior que os fornecedores podem atender; e
- Orienta a identificação e a produção de padrões relacionados ao OAIS[27].

### 4.4.3. DSS – Padrão de Assinatura Digital

O Padrão de Assinatura Digital (DSS) foi emitido em julho de 2013. Este padrão faz parte da série oficial de publicações e normas relacionadas a padrões e diretrizes adotados e promulgados sob as disposições do *Federal Information Security Management Act* (FISMA) de 2002. O nome dessa série oficial é "*The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology* (NIST)".

Este padrão define métodos para a geração de assinaturas digitais que podem ser usados para a proteção de dados binários (comumente chamados de mensagens) e para a verificação e validação dessas assinaturas digitais. Três métodos são aprovados:

- Algoritmo de Assinatura Digital DSA (do inglês, *Digital Signature Algorithm*),

---

26 **ISO 14721:2012** (Organização Internacional de Normalização, 2012)

27 Idem.

- Assinatura digital RSA (do inglês, *Rivest-Shamir-Adleman*), e
- Algoritmo de Assinatura Digital de Curva Elíptica ECDSA (do inglês *Elliptic Curve Digital Signature Algorithm*).

Além dos métodos, este padrão inclui requisitos para obter as garantias necessárias para assinaturas digitais válidas. Métodos para obter essas garantias são fornecidos na Publicação Especial (SP) 800-89 do NIST[28], intitulada "Recomendação para Obtenção de Garantias para Aplicações de Assinatura Digital". (Instituto Nacional de Padrões e Tecnologia, 2012)

### 4.4.4. Regulamento eIDAS

O Regulamento eIDAS, intitulado oficialmente "Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 sobre identificação eletrônica e serviços de confiança para transações eletrônicas no mercado interno e que revoga a Diretiva 1999/93/CE", aplica-se a todos os Estados-Membros da União Europeia desde 1º de julho de 2016. O período de transição terminou em 1º de julho de 2017, e o regulamento foi totalmente implementado, deixando os serviços de confiança de serem regulados por leis nacionais.

O Regulamento eIDAS estabeleceu regras sob as quais pessoas e instituições podem usar os meios de identificação eletrônica fornecidos por seus próprios Estados em outros Estados-Membros, além de regras para vários serviços de confiança, especialmente transações eletrônicas, e um quadro jurídico para "assinaturas eletrônicas, selos eletrônicos, carimbos de tempo eletrônicos, documentos eletrônicos, serviços de entrega eletrônica e serviços de certificação de páginas da web".

Como o regulamento eIDAS exige, entre outras coisas, que os certificados de assinatura digital sejam emitidos apenas para pessoas físicas, todos os certificados de assinatura digital emitidos para pessoas jurídicas, sob a antiga Diretiva de Assinatura Eletrônica, não podem mais ser usados para criar assinaturas digitais legalmente válidas. Pessoas jurídicas devem receber certificados de assinatura para serem usados como selos digitais. Além disso, o eIDAS exige o estabelecimento de uma lista de provedores de serviços de confiança qualificados na União Europeia (a Lista de Confiança da UE).

No que diz respeito à preservação de longo prazo de registros assinados digitalmente, o Regulamento eIDAS define carimbos de tempo eletrônicos como "informações em um meio eletrônico que criam um vínculo entre outros dados eletrônicos e um determinado momento, provando assim sua existência em um momento e data específicos". Este regulamento é esperado para ter um efeito positivo sobre empresas e indivíduos, permitindo a criação de novos serviços de confiança qualificados[29].

"O Regulamento eIDAS estabelece regras para a preservação de assinaturas eletrônicas, selos eletrônicos ou certificados relacionados a serviços de confiança. A preservação é diferente do arquivamento eletrônico (que NÃO é um serviço de confiança sob o eIDAS). Os objetivos e metas do processo distinguem as duas atividades:

A preservação sob o eIDAS visa garantir a confiabilidade de uma assinatura eletrônica qualificada ou de um selo eletrônico qualificado ao longo do tempo. A tecnologia que sustenta esse serviço de confiança, portanto, foca na assinatura eletrônica ou no selo;

O arquivamento eletrônico visa garantir que um documento seja armazenado para garantir sua integri-

---

28 O Padrão de Criptografia de Dados (DES) fazia parte dessas séries oficiais. Ele esteve em vigor de julho de 1977 até maio de 2005. Os algoritmos descritos neste padrão especificavam operações de cifragem e decifragem baseadas em um número binário chamado chave. (Instituto Nacional de Padrões e Tecnologia, 1999)

29 Regulamento eIDAS (Parlamento Europeu, 2014)

dade (e outras características legais). A tecnologia que sustenta o arquivamento eletrônico, portanto, foca no documento. O arquivamento eletrônico permanece sob a competência dos Estados-Membros.

Em outras palavras, o arquivamento eletrônico de documentos e a preservação de assinaturas eletrônicas e selos eletrônicos são diferentes em natureza, baseiam-se em soluções técnicas distintas (vinculadas ao documento ou à assinatura eletrônica/selo eletrônico) e diferem em sua finalidade (conservação do documento versus preservação da assinatura eletrônica/selo eletrônico)." (Comissão Europeia, 2016)

Curiosamente, a Comissão Europeia usa o termo conservação do documento e o diferencia do termo preservação da assinatura eletrônica, enquanto esta equipe de pesquisa acredita que, em ambos os casos, o termo preservação deveria ser usado.

#### 4.4.5. ISO/TC 307 – Blockchain e Tecnologias de Registro Distribuído

A tecnologia blockchain está em processo de padronização pela Organização Internacional de Padronização (ISO/TC 307)[30] com o objetivo de apoiar a interoperabilidade e a troca de dados entre usuários, aplicações e sistemas. A 1ª reunião foi realizada em abril de 2017. Os membros deste grupo de estudo estão ativamente envolvidos no desenvolvimento do padrão – Victoria Lemieux foi nomeada Chefe do Grupo de Trabalho de Terminologia, e Hrvoje Stančić foi nomeado Presidente do Comitê Técnico Espelho ISO/TC 307 da Croácia, junto ao Instituto de Normas da Croácia.

Em dezembro de 2017, o CEN/CENELEC criou um Grupo de Foco em Blockchain e Tecnologias de Registro Distribuído com o objetivo de identificar necessidades específicas de padronização europeia, mapear essas necessidades (incluindo a governança de blockchain e DLT no contexto do Regulamento Geral de Proteção de Dados – GDPR), em relação aos itens de trabalho atuais no ISO/TC 307, e incentivar uma maior participação europeia neste Comitê Técnico da ISO[31].

### 4.5 Abordagens atuais para arquivamento e preservação de longo prazo de registros assinados digitalmente

A preservação de longo prazo de registros digitais que são assinados digitalmente ou possuem um selo digital anexado é um desafio para a profissão arquivística. Esses registros digitais não são fáceis de preservar, não apenas devido aos constantes avanços tecnológicos, mas também porque os certificados nos quais eles se baseiam não são projetados para durar indefinidamente. Por exemplo, a Agência Financeira (FINA), uma Autoridade Certificadora (CA) na Croácia, emite certificados com um período de validade de dois anos, enquanto a Agência para Atividades Comerciais (em croata, Agencija za komercijalnu djelatnost, AKD) emite certificados com um período de validade de cinco anos (estes são usados em cartões de identidade eletrônicos). Os certificados raiz do emissor geralmente têm um período de validade mais longo, por exemplo, dez anos. Após o vencimento do período de validade do certificado, não será mais possível verificar a validade da assinatura digital usando métodos e softwares comuns, mas ainda será possível verificar a integridade do próprio registro.

Atualmente, existem várias abordagens para a preservação de longo prazo de registros digitais que possuem assinaturas ou selos digitais anexados. De acordo com o PREMIS (*Data Dictionary for Preservation Metadata*: PREMIS version 3.0, 2015), os repositórios de preservação utilizam assinaturas digitais de três maneiras principais:

1. **Para submissão ao repositório**, um agente (autor ou remetente) pode assinar um objeto para afirmar que ele é, de fato, o autor ou remetente;

---

30 ISO / TC 307, https://www.iso.org/committee/6266604.html

31 Novo Grupo de Foco do CEN e CENELEC sobre Blockchain e Tecnologias de Registro Distribuído (DLT), https://www.cencenelec.eu/news/articles/Pages/AR-2017-012.aspx

2. **Para disseminação a partir do repositório**, o repositório pode assinar um objeto para afirmar que ele é, de fato, a fonte da disseminação;
3. **Para armazenamento arquivístico**, um repositório pode querer arquivar objetos assinados para que seja possível confirmar a origem e a integridade dos dados.

Em todos os casos em que assinaturas digitais são usadas pelo repositório como uma ferramenta para confirmar a autenticidade de seus objetos digitais armazenados ao longo do tempo, a própria assinatura e as informações necessárias para validá-la devem ser preservadas (juntamente com os originais e a documentação de suporte – certificados digitais, CRLs, respostas OCSP, etc.). A revalidação das assinaturas deve ser evitada sempre que possível, até que a tecnologia de arquivamento esteja totalmente estabelecida e seja apoiada por legislação e práticas legais.

De acordo com Blanchette (Blanchette, 2006), do ponto de vista dos arquivos, existem três opções possíveis:

1. **Preservar as assinaturas digitais:** Essa solução supõe o uso de meios consideráveis para preservar os mecanismos necessários para validar as assinaturas, mas não aborda a necessidade de preservar simultaneamente a inteligibilidade dos documentos.
2. **Eliminar as assinaturas:** Essa opção exige a menor adaptação por parte das instituições arquivísticas, mas empobrece a descrição do documento, pois elimina a assinatura como um elemento técnico usado para garantir a autenticidade dos documentos[32].
3. **Registrar o traço das assinaturas como metadados:** Essa solução requer poucos recursos técnicos e registra tanto a existência da assinatura quanto o resultado de sua verificação. No entanto, as assinaturas digitais perdem seu status especial como a principal forma de evidência para inferir a autenticidade do documento. Além disso, essa abordagem exige a existência de uma terceira parte confiável para preservar e autenticar os metadados.

Outras abordagens possíveis incluem, por exemplo, o uso de registros oficiais do estado para documentos criados ou recebidos, em combinação com o arquivamento precoce. Certos autores argumentam que a única opção viável é a primeira, ou seja, preservar as assinaturas digitais para desenvolver um Serviço Arquivístico Confiável (*Trusted Archival Service - TAS*), que possa garantir que a assinatura de um registro ainda possa ser validada anos depois (Dumortier & Van den Eynde), é uma abordagem que ainda precisa alcançar uma implementação ampla.

No entanto, os resultados dos projetos anteriores do InterPARES recomendam a terceira opção, ou seja, organizar um arquivo digital de forma a verificar a validade das assinaturas digitais na fase de ingestão (seja por revalidação técnica das assinaturas ou por obtenção de garantias da autoridade relevante), adicionar as informações de validade aos metadados dos registros e preservar os registros sem abordar a validade da assinatura digital posteriormente. Assim, a questão da confiança é transferida do registro (assinado digitalmente) para o arquivo que preserva os registros digitais e os metadados associados (de validade). Isso segue o modelo mais tradicional de preservação arquivística, que contrasta com a premissa subjacente da tecnologia de blockchain e registros distribuídos, que não depende de uma terceira parte confiável ou de um intermediário de preservação. (Nakamoto, 2008)

Mais adiante neste relatório de pesquisa, mostraremos que existe uma quarta opção baseada nos princípios das tecnologias de blockchain e registros distribuídos, ou seja, registrar a validade da assinatura digital em uma blockchain.

---

32 É amplamente considerado uma má prática descartar completamente o elemento da assinatura. Dificilmente será possível convencer um tribunal de que isso foi feito de boa-fé. A eliminação é agora mais frequentemente entendida como uma recusa de uma instituição arquivística em realizar a revalidação.

### 4.5.1. OAIS e TDR

O arquivo digital estabelecido de acordo com o modelo de referência OAIS é considerado a solução tecnicamente menos exigente. Ao inserir um registro com uma assinatura digital em um arquivo digital, a validade da assinatura digital pode ser verificada, e essa informação pode ser registrada nos metadados. Após a verificação, o registro é armazenado em um pacote de informações arquivísticas (*Archival Information Package* - AIP) com os metadados associados. Dessa forma, se a informação de validade foi realmente registrada como metadado, a expiração do certificado deixa de ser tão importante, pois a informação sobre sua validade no momento da ingestão foi armazenada.

No entanto, para que se tenha confiança no arquivo digital compatível com o OAIS, ele deve ser estabelecido de acordo com a norma ISO 16363:2012 Auditoria e certificação de repositórios digitais confiáveis (*Audit and Certification of Trustworthy Digital Repositories* - TDR) (Organização Internacional de Padronização, 2012). Essa norma prescreve como diversas etapas realizadas durante a preservação de longo prazo devem ser conduzidas de forma a não comprometer a credibilidade dos registros digitais armazenados no arquivo. Em outras palavras, somente quando um arquivo digital é compatível com OAIS e TDR, ele pode ser confiável o suficiente para transferir a informação sobre a validade de uma assinatura ou selo digital do próprio registro para o arquivo digital.

### 4.5.2. CRL e OCSP

No contexto de tecnologias que contribuem para a preservação de longo prazo de registros assinados digitalmente, é necessário distinguir entre a *Certificate Revocation List – CRL* (Cooper, Santesson, Farrell, Boeyen, Housley, & Polk, 2008) e o *Online Certificate Status Protocol – OCSP* (Santesson, Myers, Ankney, Malpani, Galperin, & Adams, 2013). Ao adicionar informações sobre o status de validade do certificado a uma resposta CRL ou OCSP, e incluindo uma cadeia de certificação para garantir a confiança no certificado digitalmente assinado, é possível validar com sucesso uma assinatura digital mesmo após a expiração do certificado da assinatura.

A lista CRL é o método usual para revogar um certificado. A própria lista CRL representa um arquivo padrão com uma série de números de série. Cada certificado digital possui um número único, de modo que, se ele for encontrado na lista, significa que o certificado digital foi revogado. A CRL é publicada pela Autoridade Certificadora (CA) apropriada em intervalos de tempo predeterminados. No entanto, essa é uma desvantagem das CRLs, pois elas não funcionam como um serviço em tempo real. Por outro lado, uma vez obtida, a CRL pode ser usada sem a necessidade de estabelecer uma conexão online até que a CA emita uma nova versão. Os campos obrigatórios cruciais para a verificação posterior de assinaturas digitais são o número de série, a data e a hora da revogação do certificado digital.

O serviço OCSP é baseado no protocolo OCSP, desenvolvido devido à necessidade de superar as limitações relacionadas às CRLs. No contexto da infraestrutura de PKI, o OCSP é responsabilidade da Autoridade de Validação (*Validation Authority - VA*), que valida os certificados digitais. No caso de uso do OCSP, a Autoridade Certificadora (CA) envia as informações sobre a revogação do certificado digital para a VA. Uma pessoa ou serviço que deseja verificar a validade de um certificado digital envia uma consulta à VA e recebe uma resposta como “válido”, “revogado” ou “desconhecido”.

Portanto, ao usar o OCSP, não é necessário baixar a CRL e salvá-la junto com os registros arquivados, bastando estabelecer uma comunicação direta com a VA para verificar se um certificado digital é válido. Ao mesmo tempo, essa é a principal desvantagem – a perda da conexão com a Internet impossibilita a verificação da validade.

### 4.5.3. Carimbo de Tempo Arquivístico

Além do carimbo de tempo padrão, existe um tipo especial de carimbo de tempo destinado à preservação de longo prazo – o carimbo de tempo arquivístico (*archival timestamp*) ou token de carimbo de tempo para a disponibilidade e integridade de longo prazo do material de validação. Ele não difere de um carimbo de tempo padrão nem teoricamente nem tecnicamente, mas apenas em seu escopo. Ele inclui uma série de valores de *hash* – um para cada pedaço de informação que precisa ser mantido e vinculado por um longo período. O objetivo principal do carimbo de tempo arquivístico é estender a validade da assinatura digital e permitir uma resposta positiva de CRL ou OCSP à verificação de validade, mesmo após o período de validade dos certificados de assinatura.

O carimbo de tempo arquivístico implementa um princípio de encapsulamento em camadas, semelhante a uma cebola. A norma ETSI EN 319 102-1 Procedures for *Creation and Validation of AdES Digital Signatures*; Part 1: Creation and Validation define quatro níveis básicos de assinaturas digitais de base, permitindo a interoperabilidade e o ciclo de vida dos registros. Cada nível encapsula todas as informações dos níveis anteriores. Os níveis são:

- B-B – básico,
- B-T – carimbo de tempo adicionado ao nível B,
- B-LT – informações de verificação de validade de longo prazo adicionadas ao nível T, e
- B-LTA – permite a adição periódica do carimbo de tempo arquivístico ao nível LT (Figura 1). (ETSI, 2016)

Na prática, isso significa que o sistema de preservação de longo prazo deve ser configurado de forma a verificar o período de expiração dos certificados de cada registro assinado digitalmente ou a expiração de um carimbo de tempo arquivístico já adicionado e (re)aplicar o carimbo de tempo arquivístico (B-LTA) antes que os certificados de assinatura ou o carimbo de tempo arquivístico previamente adicionado expirem. Isso, é claro, pode representar um desafio para os arquivos digitais que preservam grandes coleções de registros assinados digitalmente.

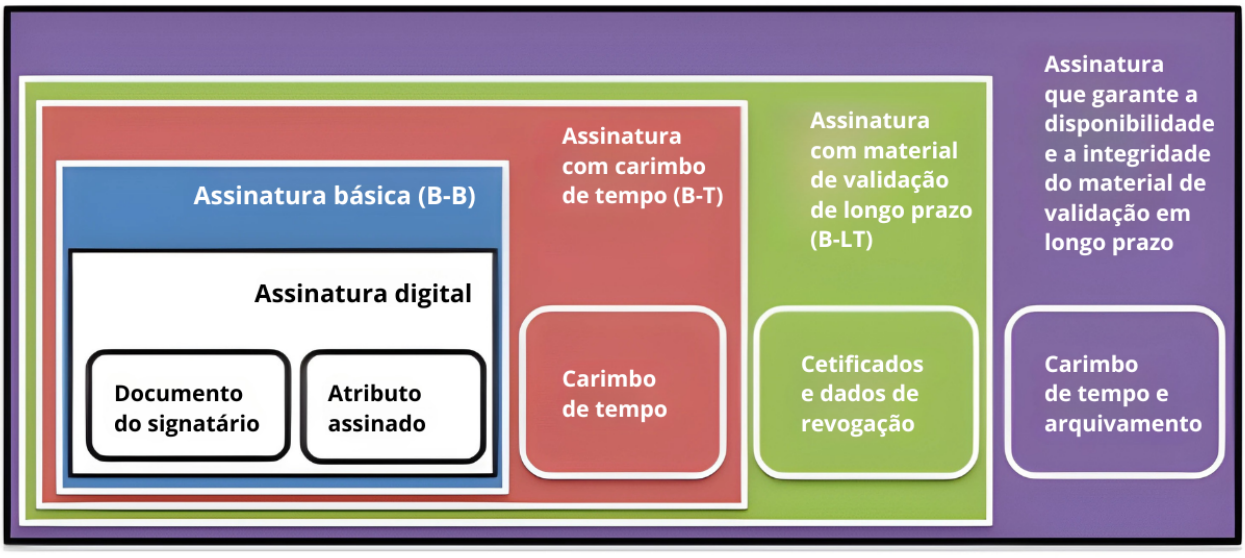


Figura 10: Carimbo de Tempo Arquivístico

## 5. Questões de Pesquisa

1. As questões levantadas pela equipe de pesquisa no início do estudo foram:
2. Por que os registros assinados digitalmente, com carimbo de tempo ou selados devem ser preservados?
3. Eles ainda possuem algum valor comercial ou histórico que justifique os custos?
4. Existe a necessidade de revalidar certificados digitais já expirados e como isso pode ser feito?
5. Existem bancos de dados oficiais contendo as informações dos registros?
6. Os certificados digitais podem ser renovados aplicando carimbos de tempo nos certificados encapsulados antes de sua expiração?
7. Existem outras maneiras de manter as assinaturas válidas a longo prazo?
8. Em quais situações é importante exigir um carimbo de tempo?
9. Podemos presumir a confiabilidade do momento de criação se ele for registrado fora do ambiente controlado do arquivo digital?
10. Podemos presumir a confiabilidade de assinaturas digitais que não possuem informações de revogação incorporadas, ou podemos presumir a confiabilidade da assinatura digital do servidor de ingestão se ela não tiver um carimbo de tempo?
11. Existem maneiras legais existentes de autenticar o conteúdo dos registros sem revalidar as assinaturas originais?
12. É possível não fazer nada ou usar soluções que não sejam exatamente 100% compatíveis com a legislação? Quais poderiam ser as consequências?
13. Existe a necessidade de alterar as leis e regulamentos?
14. Usando a tecnologia contemporânea, é possível desenvolver sistemas que proporcionem confiança em assinaturas digitais e certificados por períodos mais longos?

## 6. Objetivos e Metas

Os objetivos do estudo de pesquisa:

1. Abordar uma questão arquivística importante sobre a preservação de registros digitais na nuvem, utilizando novos conceitos tecnológicos, como a blockchain.
2. Construir um modelo que sugira como preservar a confiabilidade dos registros digitais com assinaturas digitais, certificados, carimbos de tempo ou selos adicionados a eles.
3. Investigar as possibilidades de revalidação de assinaturas digitais expiradas, atualização da assinatura periódica de registros digitais, renovação de carimbos de tempo, adição de carimbos de tempo arquivísticos, injeção de provas adicionais (com carimbo de tempo) de existência, entre outros.

As metas do estudo de pesquisa:

1. Obter resultados que possam ser usados para elaborar e/ou melhorar estruturas regulatórias.
2. Obter resultados que possam ser usados para elaborar e/ou melhorar políticas e procedimentos organizacionais internos.
3. De forma geral, alcançar resultados relevantes para a organização e o desenvolvimento de serviços arquivísticos confiáveis, baseados na ingestão de registros confiáveis.

## 7. Metodologia

Para alcançar os objetivos e metas estabelecidos, a pesquisa foi dividida em cinco fases ao longo de 19 meses (março de 2016 – setembro de 2017).

Na primeira fase, a equipe utilizou uma abordagem comparativa para revisar a literatura existente nos campos de arquivamento, estrutura legal, blockchain e tecnologias de registros distribuídos.

Na segunda fase, foram desenvolvidos três casos. Esses casos investigaram os procedimentos e desafios em situações reais de preservação de longo prazo de registros assinados digitalmente em serviços públicos.

Na terceira fase, que ocorreu simultaneamente à segunda, diversos casos de uso de gestão de registros e preservação arquivística foram investigados durante o desenvolvimento dos estudos de caso.

Com base nisso, na quarta fase, foi desenvolvido o modelo para preservação da validade de registros assinados digitalmente e com carimbo de tempo (Solução *TRUSTER VIP – Validity Information Preservation: TrustChain*). O modelo fornece uma estrutura para um sistema que poderia permitir aos arquivos preservar a autenticidade (informações do certificado ou, pelo menos, informações de validade do certificado) e a integridade (usando assinaturas digitais) de documentos assinados digitalmente.

A quinta e última fase da pesquisa consistiu na redação deste relatório (Figura 11).

InterPARES Trust

**Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31)**

| | 2016 | | | | | | | | | | 2017 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | MAR | APR | MAY | JUN | JUL | AUG | SEP | OCT | NOV | DEC | JAN | FEB | MAR | APR | MAY | JUN | JUL | AUG | SEP |
| | M1 | M2 | M3 | M4 | M5 | M6 | M7 | M8 | M9 | M10 | M11 | M12 | M13 | M14 | M15 | M16 | M17 | M18 | M19 |
| **Phase 1 - review of the relevant literature** | | | | | | | | | | | | | | | | | | | |
| | FHSS | | | | | | | | | | | | | | | | | | |
| | IE | | | | | | | | | | | | | | | | | | |
| | UBC | | | | | | | | | | | | | | | | | | |
| **Phase 2 - development of case studies** | | | | | | | | | | | | | | | | | | | |
| | | | | T | | | | | | | | | | | | | | | |
| | | | | F | | | | | | | | | | | | | | | |
| | | | | E | | | | | | | | | | | | | | | |
| **Phase 3 - testing of various recordkeeping and archival preservation use cases** | | | | | | | | | | | | | | | | | | | |
| | | | | FHSS | | | | | | | | | | | | | | | |
| | | | | E | | | | | | | | | | | | | | | |
| | | | | UBC | | | | | | | | | | | | | | | |
| **Phase 4 - development of the model for preservation of validity of digitally signed and timestamped records** | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | FHSS | | | | | | | | | | |
| | | | | | | | | | T | | | | | | | | | | |
| | | | | | | | | | F | | | | | | | | | | |
| | | | | | | | | | E | | | | | | | | | | |
| | | | | | | | | | IE | | | | | | | | | | |
| | | | | | | | | | UBC | | | | | | | | | | |
| **Phase 5 - write a report** | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | FHSS | | | |
| | | | | | | | | | | | | | | | | T | | | |
| | | | | | | | | | | | | | | | | F | | | |
| | | | | | | | | | | | | | | | | E | | | |
| | | | | | | | | | | | | | | | | IE | | | |
| | | | | | | | | | | | | | | | | UBC | | | |
| **Conference call meetings (using Victoria Lemieux's access to "GoToMeeting")** | | | | | | | | | | | | | | | | | | | |
| Conference calls | | X | | X | | | X | | X | | X | | X | | X | X | | X | X |
| | | | | | | | | | | | | | | | | | | | |
| Milestones | | M1 | | M2 | | M3 | | | M4 | | | M5 | | M6 | | M7 | | M8 | |
| Result | | | R1 | | | | R2 | | R3 | | | | | | R4 | | | | FR |
| **Meetings and dissemination** | | | | | | | | | | | | | | | | | | | |
| EU Team meetings (Marburg, Oslo, Girona) | | | | 8.-10. | | | | 24.-26. | | | | | | | 11.-12. | | | | |
| Plenary meeting (Rio) | | | | | | | | | | | | 20.-22. | | | | | | | |

| | |
|---|---|
| M | Milestone |
| R | Result (FR = Final Result) |
| FHSS | FHSS |
| T | Teched |
| F | Fina |
| E | Enigio |
| IE | Independent Expert |

Figura 11: Cronograma da pesquisa

# 8. Resultados

Os resultados são divididos em duas seções – a primeira descreve os resultados dos estudos de caso, que estão disponíveis como produtos independentes, e a segunda apresenta o modelo de sistema de informação *TrustChain* para a preservação de longo prazo de registros assinados digitalmente.

## 8.1 Estudos de Caso

Em cooperação com três parceiros envolvidos, FINA (Croácia), TechEd (Croácia) e Enigio Time (Suécia), três estudos de caso foram desenvolvidos. Cada um desses três parceiros tinha acesso a registros assinados digitalmente com assinaturas digitais expiradas ou com expiração próxima. Os estudos de caso conduzidos exploraram como várias instituições financeiras, do setor público e médicas lidam com a preservação de longo prazo de registros assinados digitalmente.

No decorrer da pesquisa, um questionário foi desenvolvido e utilizado para tornar os resultados dos estudos de caso comparáveis. Ele foi usado nos estudos de caso 1 e 2. O questionário pode ser encontrado no Apêndice 1 deste relatório.

Os principais objetivos dos estudos de caso foram (1) analisar o uso atual e o estado de preservação de registros assinados digitalmente mantidos por diferentes instituições, (2) compreender o valor percebido da necessidade de arquivamento das assinaturas digitais, bem como o arquivamento da validade das assinaturas digitais, e (3) compreender como a expiração dos certificados em assinaturas digitais poderia influenciar a admissibilidade dos registros como prova no tribunal.

Em geral, a análise dos estudos de caso se concentrou nos registros assinados digitalmente e na preservação da validade dos certificados utilizados em vários casos de uso de gestão de registros e preservação arquivística. Assim, os estudos de caso resumem os procedimentos com esses registros relacionados aos objetivos do estudo de caso. Eles também podem funcionar como base para uma maior cooperação ou estudos adicionais mais detalhados.

Os textos completos dos estudos de caso estão disponíveis como produtos independentes. Aqui, apenas informações breves sobre os estudos de caso são fornecidas.

### 8.1.1. Estudo de Caso 1 – Registros de fundos de aposentadoria assinados digitalmente

Este estudo de caso foi realizado em cooperação com a FINA – Agência Financeira da Croácia, entre junho e outubro de 2016.

O estudo investigou os processos relacionados a registros assinados digitalmente no sistema e-Regos, que foi desativado e transferido para a FINA como um serviço terceirizado. A pesquisa mostrou que os registros no sistema e-Regos utilizavam assinaturas qualificadas e carimbos de tempo da FINA (uma Autoridade Certificadora na Croácia). Antes da desativação do sistema e-Regos, os registros foram transferidos para a FINA, que agora armazena os registros digitais originais localmente, ou seja, eles não estão acessíveis online. No entanto, as informações dos registros foram transferidas para um banco de dados online, onde estão acessíveis. As assinaturas digitais nos registros originais não podem mais ser validadas, pois as CRLs e as cadeias de certificados da época não foram preservadas.

O estudo destaca a necessidade de desenvolver uma estratégia de preservação digital e uma política para a preservação da validade das assinaturas digitais. Também foi observado que, neste caso específico, uma solução organizacional é possível – a obrigação legal de preservação pode ser transferida para um banco de dados, e os registros originais assinados digitalmente podem ser descartados, já que não possuem valor legal ou comercial duradouro.

Essa abordagem é direta e não exige inovações técnicas, mas, antes do descarte dos documentos originais, será necessário atualizar a legislação e os regulamentos, o que pode se mostrar um desafio.

### 8.1.2. Estudo de Caso 2 – Registros de *e-tax* assinados digitalmente

Este estudo de caso foi realizado em cooperação com a TechEd Consulting Ltd. e a Administração Tributária da Croácia, entre janeiro e abril de 2017.

O estudo investigou os processos relacionados a registros assinados digitalmente sob a custódia da Administração Tributária da Croácia. A pesquisa mostrou que os registros possuem assinaturas XML, assinaturas qualificadas e carimbos de tempo. As assinaturas digitais nos registros originais datados de 2006 não podem mais ser validadas, pois expiraram.

Para verificá-las, a Administração Tributária precisaria solicitar à Autoridade Certificadora (CA) que originalmente emitiu as chaves para as assinaturas digitais que fornecesse as CRLs antigas e as cadeias de certificados daquele período. No entanto, essas informações não foram preservadas. Nem as informações sobre a validade das assinaturas digitais, nem outras informações relacionadas às assinaturas digitais foram registradas como metadados33.

### 8.1.3. Estudo de Caso 3 – Registros médicos assinados digitalmente, contratos de aquisição e fornecedores, decisões políticas oficiais e atas de reuniões

Este estudo de caso foi realizado em cooperação com a Enigio Time e a Região de Skåne (Suécia), entre junho e novembro de 2016.

O estudo concentrou-se nos registros mais importantes e de maior volume que utilizam assinaturas digitais na Região de Skåne – registros médicos assinados digitalmente, contratos de aquisição e fornecedores, decisões políticas oficiais e atas de reuniões. Os registros médicos são o maior tipo de registro criado e gerenciado pela Região de Skåne, representando cerca de 80% dos registros armazenados no Arquivo da Região.

Assinaturas digitais de diversos tipos são usadas de várias maneiras em todos os tipos de registros e sistemas. O valor da preservação não foi totalmente reconhecido ou claramente definido nos fluxos de trabalho. Quando um registro assinado digitalmente é arquivado, a validade da assinatura digital não é verificada. As informações da assinatura digital são salvas como metadados. Os registros são mantidos no sistema de origem apenas para o caso de a assinatura ser necessária para verificação. Não foi identificada nenhuma outra estratégia expressa ou processo proprietário capaz de recuperar ou comprovar a validade da assinatura na Região de Skåne.

O estudo desencadeou discussões sobre a necessidade de uma análise mais focada e do desenvolvimento de uma estratégia comum para a preservação da validade das assinaturas digitais.

## 8.2 Solução TRUSTER VIP (*Validity Information Preservation*): *TrustChain*

### 8.2.1. Introdução

A solução *TRUSTER VIP TrustChain* é a quarta abordagem para preservação de longo prazo de registros digitais que têm assinaturas digitais ou selos anexados a eles (cf. capítulo 3.5. deste relatório). O modelo por trás do *TrustChain* permite que arquivos e outras instituições que lidam com registros assinados ou selados digitalmente evitem ter que assinar novamente (ou registrar com carimbo de data/hora) registros periodicamente, antes que seus certificados digitais expirem.

---

33 A autenticidade de todo o conjunto de registros pode ser estabelecida por um tribunal com base nas evidências circunstanciais disponíveis. Essa é uma prática comum em países de *common law*, o que, infelizmente, não é amplamente adotado em países de direito continental.

Para resumir brevemente o que foi explicado anteriormente, as assinaturas digitais dependem do conceito de infraestrutura de chave pública (PKI) que permite aos usuários criarem um *hash* de um documento (uma assinatura) usando uma chave privada (e secreta). Uma vez feito isso, qualquer um pode confirmar que o documento foi realmente assinado usando aquela chave privada, recalculando o *hash* usando uma chave pública conectada à chave privada (e seu proprietário no caso de assinaturas digitais avançadas). O propósito de uma assinatura digital é duplo. Primeiro, ela garante a integridade dos dados, ou seja, uma assinatura digital pode ser usada para confirmar que um documento não foi violado após ter sido assinado digitalmente. Segundo, ela pode ser usada para identificar a pessoa ou instituição (no caso de selos digitais) que o assinou. Essas informações (a conexão entre um signatário e uma identidade real) são armazenadas no certificado digital que é emitido por uma autoridade de certificação (CA). Esses certificados têm uma vida útil limitada. Quando um certificado chega ao fim de sua vida útil, ele não pode mais ser usado para identificar o signatário por métodos e softwares comuns e, dependendo dos requisitos do documento ou da instituição que o arquiva, pode precisar ser renovada ou ter registro de data e hora. A expiração do certificado é uma necessidade devido aos padrões de segurança em evolução, desenvolvimento da tecnologia da informação que, com o tempo, enfraquece a força da chave e a possibilidade de que as chaves sejam comprometidas.

Os resultados dos estudos de caso demonstraram uma grande necessidade de um sistema padronizado para manutenção de registros de longo prazo ou arquivamento de registros assinados ou lacrados digitalmente. Enquanto os padrões da indústria abordam esse problema confiando nos serviços de carimbo de data/hora34, sua solução sofre de um problema semelhante ao das próprias assinaturas digitais. Os carimbos de data/hora podem ser descritos como assinaturas digitais que apenas garantem a integridade dos dados de uma perspectiva temporal. A maioria dos serviços de carimbo de data/hora são esquemas baseados em vinculação ou soluções baseadas em PKI. Um "carimbo de data/hora" baseado em PKI inclui um *hash* do documento com carimbo de data/hora, hora do carimbo e é, na maioria das vezes, assinado com a chave privada do serviço de carimbo de data/hora. Portanto, é evidente que esse sistema sofre da mesma limitação tecnológica de vida útil que a assinatura digital em si, embora geralmente seja muito mais longa (5 a 20 anos). O documento com carimbo de data/hora precisará ser carimbado novamente após um certo período – logo antes do certificado usado pelo serviço de carimbo de data/hora expirar, o algoritmo criptográfico usado se tornar obsoleto ou antes que sua chave privada seja comprometida (claro, altamente incerto se e quando). Também deve ser observado que alguns serviços de carimbo de data/hora usam uma chave pública sem um certificado sob um esquema de chave transitória35. Enquanto a ausência de um certificado e a segurança inerente às chaves temporárias fazem com que os carimbos de data/hora pareçam ter uma vida útil ainda mais longa (possivelmente ilimitada), tais abordagens ainda não suportam a preservação do certificado e dependem da segurança da lista de chaves persistentes. Por outro lado, os esquemas baseados em vinculação são um pouco semelhantes ao modelo *TrustChain*, mas geralmente não verificam a validade do certificado e, portanto, apenas garantem a integridade dos dados.

O conceito do *TrustChain* foi publicado no artigo da conferência INFuture2017 "Um modelo para preservação de longo prazo da validade da assinatura digital: *TrustChain*" (Bralić, Kuleš e Stančić, 2017). No entanto, o modelo ainda está em uma fase conceitual inicial e será desenvolvido ainda mais. Portanto, o modelo a ser encontrado neste relatório é uma evolução do modelo apresentado no artigo original. O conceito básico do modelo é o mesmo, mas é refinado no nível de detalhes técnicos.36

Na próxima fase, esperamos um maior refinamento do modelo e desenvolvimento de protótipos funcionais do sistema. Uma vez que isso tenha sido alcançado, podemos prosseguir para reconhecer e recrutar instituições interessadas em usar o sistema *TrustChain* e manter a infraestrutura que ele requer.

---

34 6 ISO/IEC 18014-3 (I*nternational Organization for Standardization*, 2009) and ETSI 319 422 (ETSI, 2016).

35 Conforme descrito no padrão ANSI ASC x9.95 (*American National Standards Institute*, 2016).

36 A pesquisa também faz parte da tese de doutorado de Vladimir Bralić.

### 8.2.2. O modelo *TrustChain*

O objetivo do *TrustChain* é permitir que instituições de arquivo (ou outras com necessidades semelhantes) evitem a necessidade de re-assinar (ou aplicar carimbo de tempo) periodicamente todos os registros digitais assinados que estão arquivados. Nossa visão é de que o *TrustChain*, uma solução baseada em blockchain, seja mantido por uma aliança internacional de instituições de arquivo. O sistema também poderia ser implementado por uma única instituição, mas, nesse caso, o grau de segurança na validade das assinaturas seria significativamente reduzido.

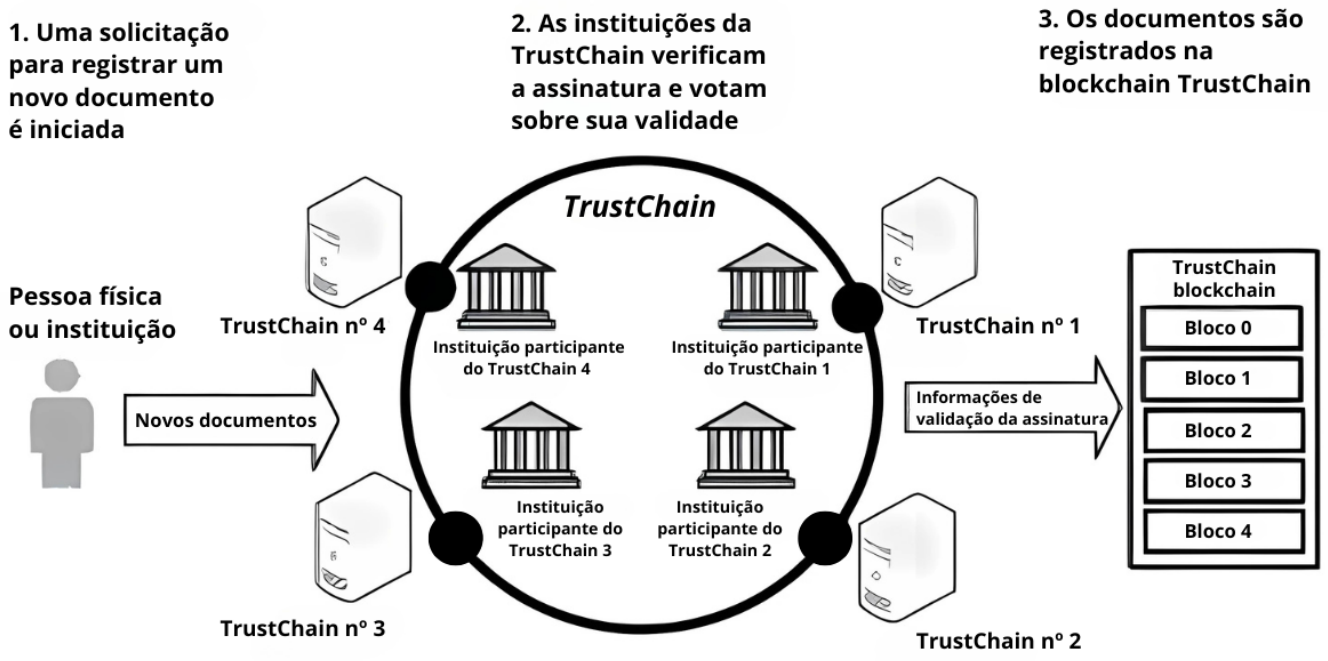


Figura 12: Conceito de *TrustChain*

**O *TrustChain* atinge o objetivo proposto verificando a validade da assinatura do documento e, se válida, gravando o hash dessa assinatura (e possivelmente alguns metadados do documento) na blockchain**. A validade da assinatura é verificada por todas ou, se o número delas for suficientemente grande, por algumas das instituições participantes. Caso a assinatura seja considerada válida, as informações são permanentemente armazenadas na blockchain do *TrustChain* (Figura 12). O processo de registro de um documento no *TrustChain* é ilustrado na Figura 13 (Bralić, Kuleš, & Stančić, 2017).

Provavelmente, a blockchain em si seria um registro (ledger) publicamente disponível e qualquer pessoa poderia lê-la. Entretanto, caso as instituições participantes desejem, a blockchain pode certamente ser um ledger permissionado, disponível apenas para nós (nodes) autorizados. O registro de novos dados, documentos ou registros na blockchain também poderia ser uma opção publicamente disponível, ou limitada apenas às instituições participantes, ou ainda oferecida comercialmente, cobrando-se uma taxa de processamento pelos nós do *TrustChain*.

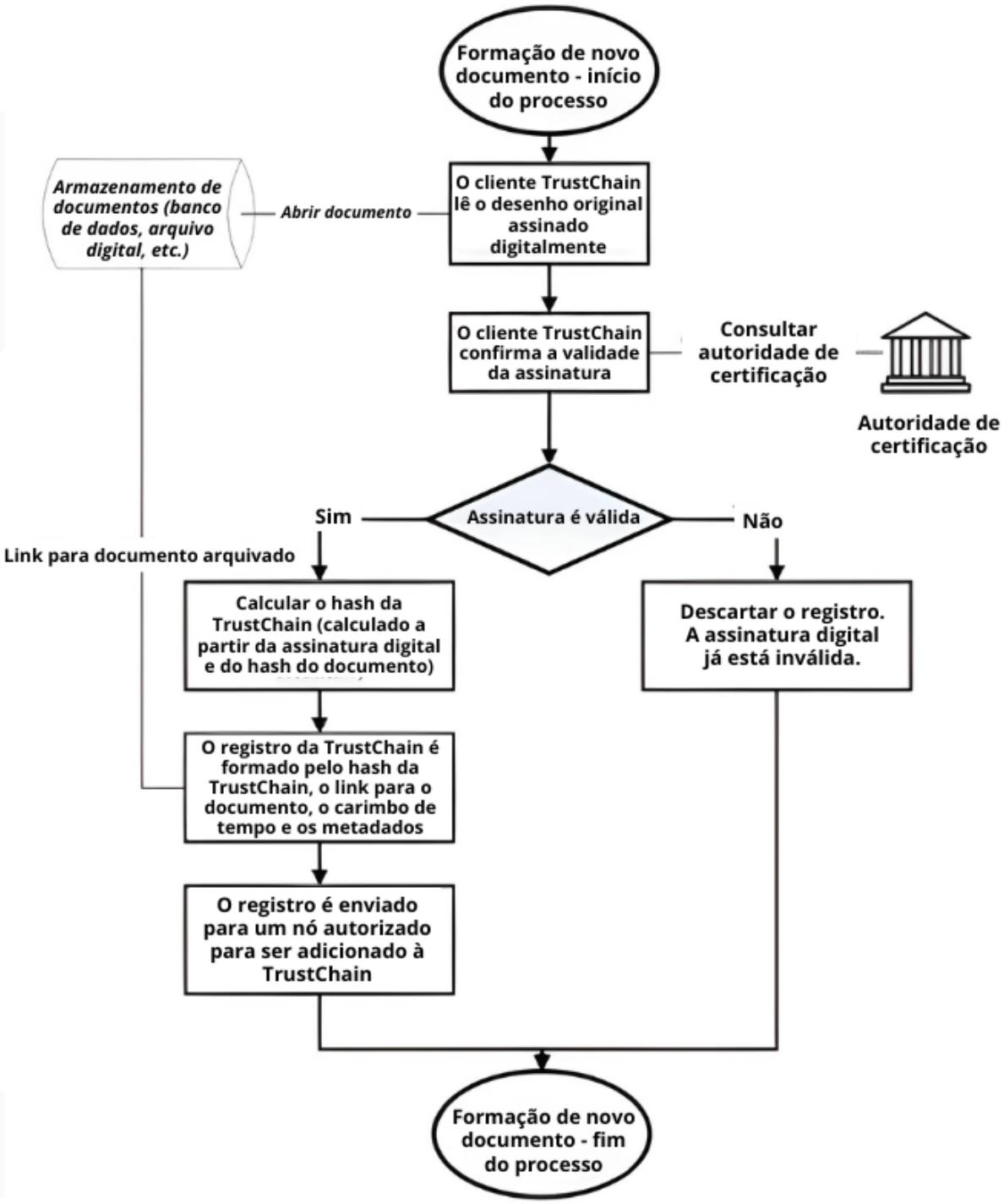


Figura 13: Registro de um documento no *TrustChain*

Ter as informações de validade de assinatura escritas em uma blockchain imutável fornece evidências de que a assinatura era válida no momento de criação do registro no *TrustChain* e de que nem o registro (conforme assegurado pela assinatura) nem a entrada na blockchain foram adulterados desde então. Essa estrutura é ilustrada na Figura 14. Devido ao fato de cada bloco conter o *hash* do bloco anterior, é impossível alterar uma parte de um bloco anterior sem reescrever todos os blocos subsequentes. Além disso, o *hash* do bloco anterior é registrado como parte das informações de votação, o que significa que essas informações de votação também são protegidas por *hash*. Os votos são formados por meio de uma chave privada pertencente aos nós que votam em um bloco.

Um invasor que deseje alterar as informações escritas na blockchain precisaria mudar todos os blocos subsequentes e, para conseguir isso, teria de obter acesso às chaves privadas de todas as instituições participantes que tenham votado nos blocos depois daquele que está sendo alterado. Dependendo do número de instituições participantes, isso pode ser praticamente impossível. É por isso que o *TrustChain* é considerado mais seguro com mais instituições participantes. Além de aumentar o número de chaves privadas que teriam de ser comprometidas, a diversidade de instituições que participam do processo de votação também fornece maior confiança de que a assinatura, de fato, era válida no momento em que foi adicionada ao *TrustChain*.

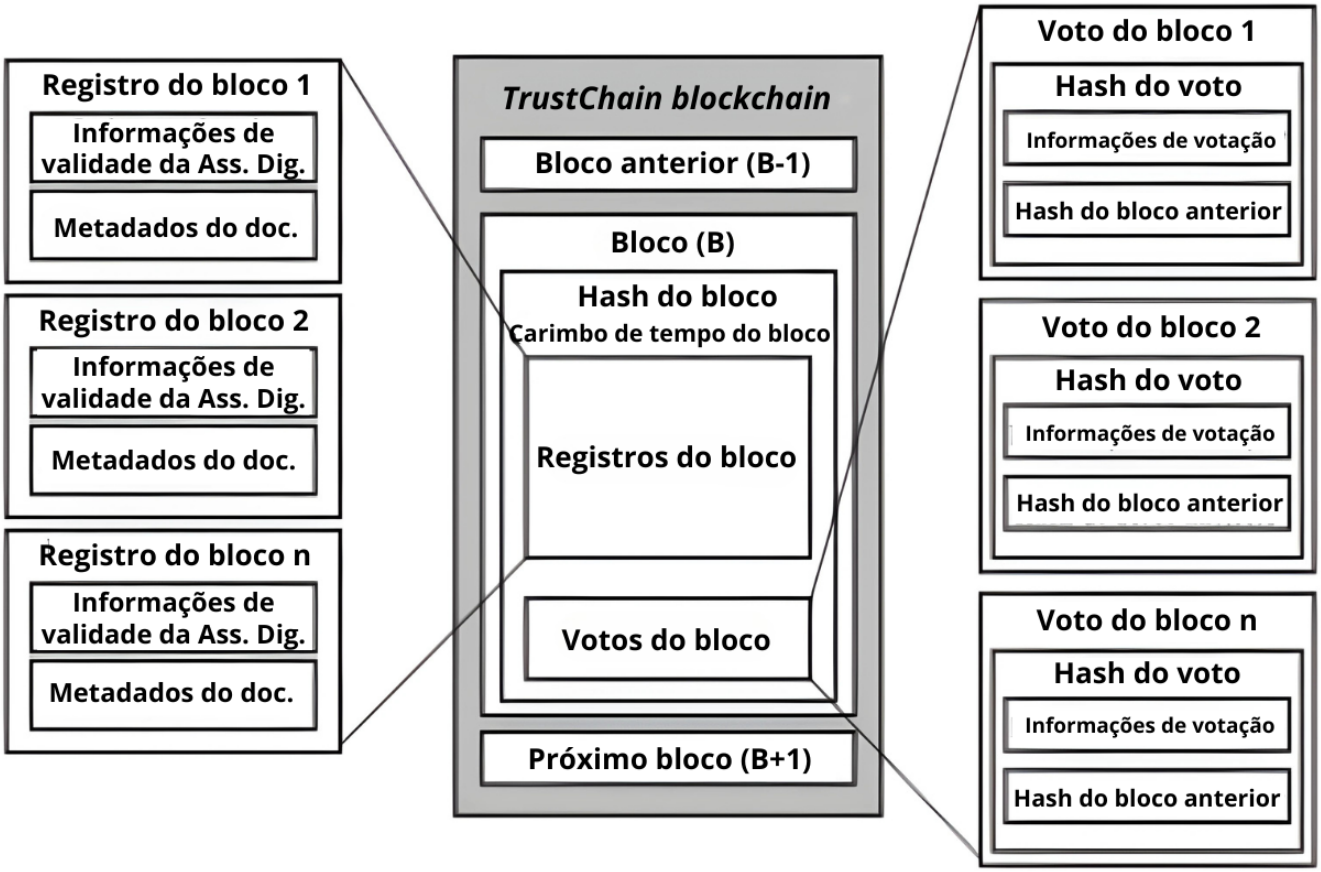


Figura 14: Estrutura de blockchain no *TrustChain*

Apesar de, assim como em outros métodos alternativos (como carimbo do tempo), o *TrustChain* depender fortemente do conceito de PKI (infraestrutura de chaves públicas) e, portanto, dos algoritmos de criptografia assimétrica, **não há necessidade de re-assinar periodicamente os dados** por causa da forma como esses dados são armazenados. A estrutura de dados em blockchain do *TrustChain* é o que lhe permite evitar os problemas de chaves privadas comprometidas ou algoritmos criptográficos obsoletos. Uma vez que um algoritmo se torne obsoleto, os nós de votação do *TrustChain* precisam apenas mudar o algoritmo que utilizam para assinar seus votos. Blocos assinados com uma chave comprometida ou obsoleta não precisam ser reassinados. Se um invasor tentasse reassiná-los com dados alterados, teria novamente de alterar e re-assinar todos os blocos subsequentes também e, em algum momento, se depararia com um bloco assinado por uma chave não comprometida (e com um algoritmo seguro). Em suma, podemos dizer que (assim como em outros modelos de dados encadeados) adicionar um novo bloco ao *TrustChain* re-assina (ou revalida) todos os registros existentes ou que a cadeia inteira (de blocos) é tão forte quanto seu elo mais forte, que, no nosso caso, será sempre o bloco mais recente (Figura 15).

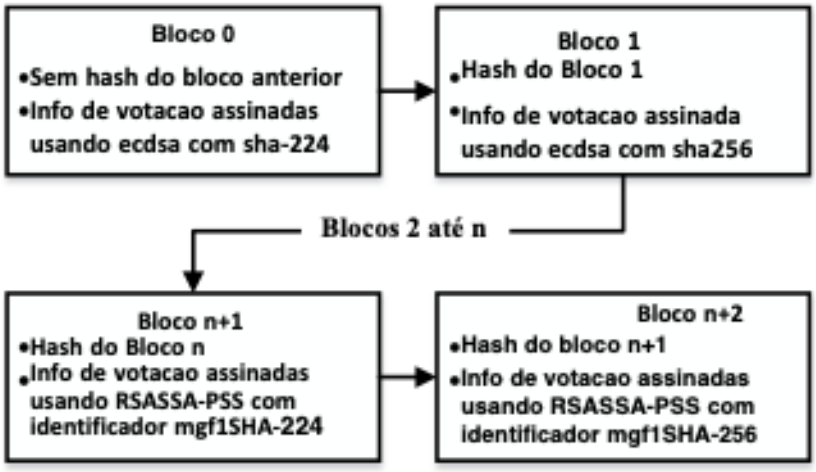


Figura 15: Mudanças no algoritmo de voto do *TrustChain*

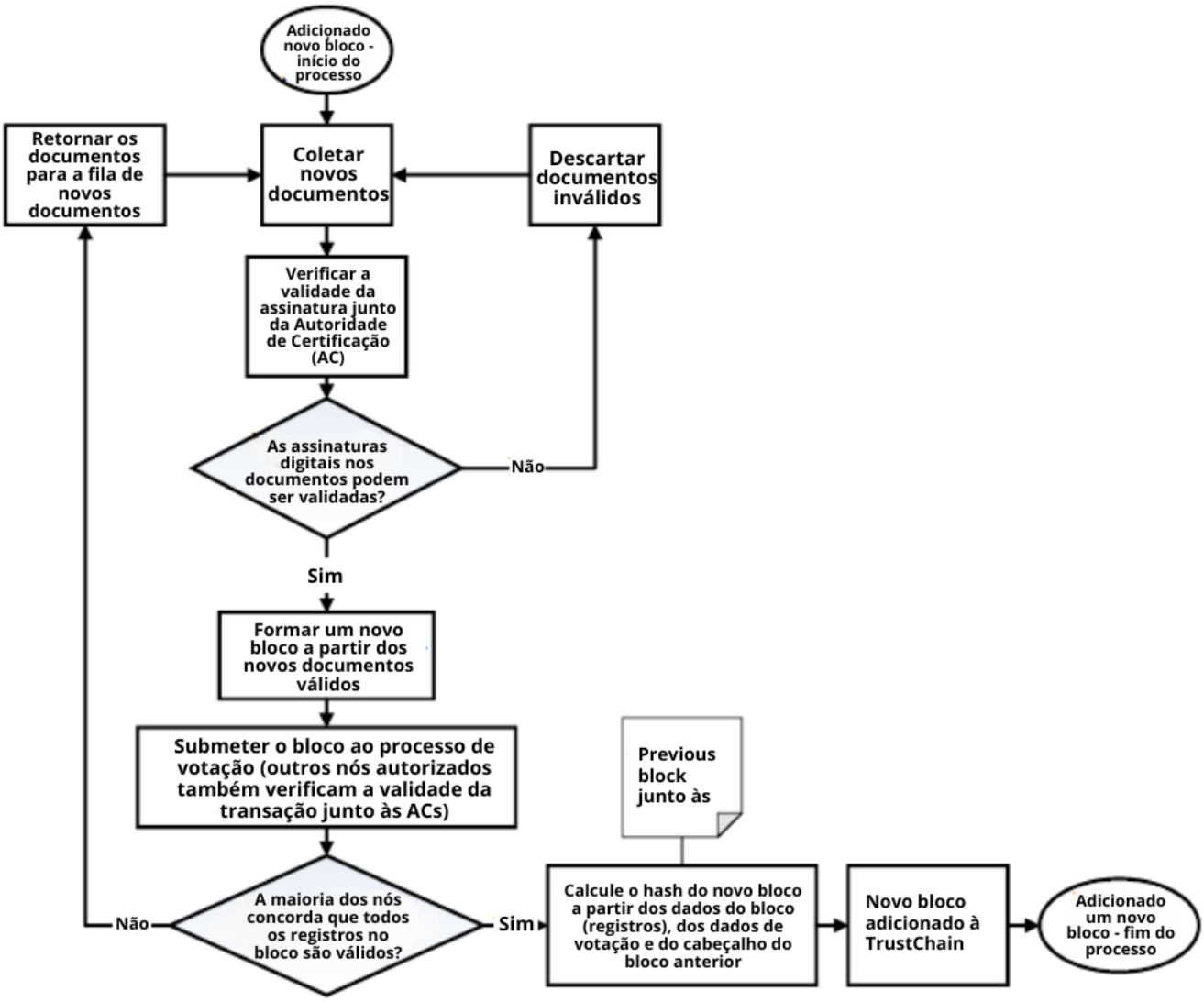


Figura 16: Adicionando um novo bloco ao *TrustChain*

O processo de adicionar registros a um bloco e gravar esse bloco na blockchain é deixado exclusivamente para os nós do *TrustChain*. Os nós coletam novos registros (candidatos) de uma fila e tentam validar todas as assinaturas. Se uma assinatura falhar, o registro é descartado como inválido e novos registros são coletados. Uma vez encontrada uma quantidade suficiente de registros válidos, eles são adicionados a um bloco, mas somente depois de outros nós confirmarem a validade das assinaturas desses registros. O número necessário depende do número total de nós disponíveis no *TrustChain* e do nível de confiabilidade exigido (quanto mais nós conferindo os registros, mais confiável será a votação). Como o número de instituições participantes não é conhecido neste estágio inicial, presumimos que todas as instituições participantes mantenham um nó e que todas votem em cada bloco. Se o número de instituições aumentar a tal ponto que seria inviável todas elas votarem em cada bloco, um subconjunto menor, selecionado aleatoriamente, poderia votar em cada bloco. Esse subconjunto deveria mudar a cada bloco. Se a maioria dos nós votantes concordar que o bloco é válido, ele pode ser adicionado à blockchain (após ter seu *hash* calculado a partir de seu conteúdo e do *hash* do bloco anterior). Caso contrário, o bloco é descartado e os registros que o formaram retornam para a fila de novos registros (Figura 16). (Bralić, Kuleš, & Stančić, 2017)

O processo de confirmação das assinaturas digitais (expiradas) começa localizando os registros relevantes na blockchain do *TrustChain*. Para isso, o *TrustChain* depende dos metadados do documento gravados – o conjunto de elementos essenciais do ISAD(G), mas que também podem conter informações relativas ao vínculo arquivístico (archival bond) (Lemieux & Sporny, 2017). Uma vez identificado o registro relevante, tudo o que precisa ser feito é recalcular o *hash* a partir do documento original e compará-lo com aquele gravado no *TrustChain*. Se esses *hashes* forem iguais, pode-se afirmar com segurança que o documento e sua assinatura permaneceram inalterados desde a data indicada pelo registro de data/hora (carimbo do tempo) na blockchain (Figura 17). (Bralić, Kuleš, & Stančić, 2017)

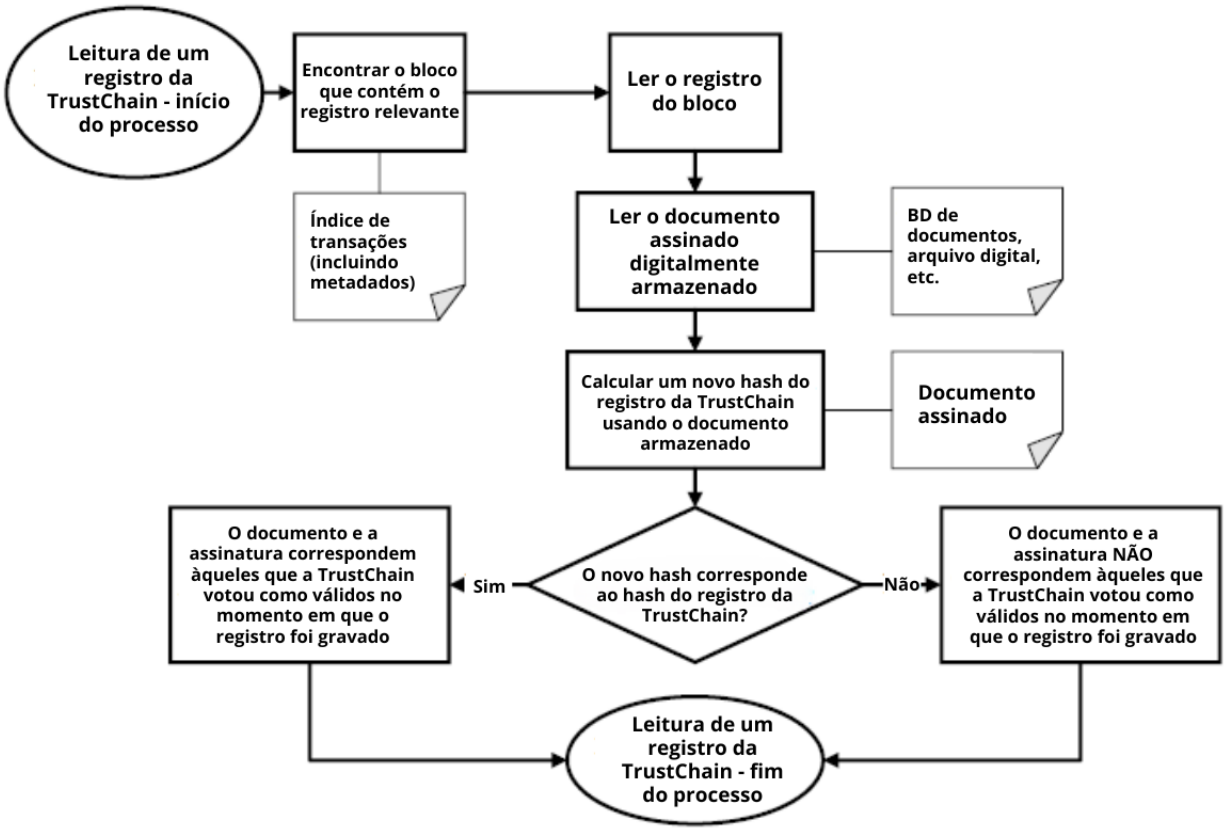


Figura 17: Lendo um registro do *TrustChain*

## 8.3 Discussão

O modelo atual do *TrustChain* detalhado aqui foi discutido pelos pesquisadores do InterPARES Trust (aqueles que não participam diretamente do desenvolvimento do modelo) e pela plateia e revisores da conferência INFuture2017. Vários pontos levantados serão abordados em seguida.

Em primeiro lugar, há opiniões contrárias em relação à inclusão de metadados na blockchain. Por um lado, é conveniente ter parte dessas informações escritas diretamente na blockchain para permitir a pesquisa nela. Sem isso, a pesquisa seria possível apenas pelos *hashes*, ou seja, somente aqueles que possuem o *hash* do documento poderiam identificá-lo na cadeia, enquanto os demais não conseguiriam. Escrever metadados na blockchain apoia a abertura do sistema e possibilita que qualquer pessoa confirme seu conteúdo. Por outro lado, não escrever metadados estimula a privacidade na blockchain, o que pode ser importante para determinados usuários, como bancos ou outras instituições financeiras. Uma das possíveis soluções para isso é criar diferentes tipos de metadados de acordo com ontologias específicas para certos tipos de documento. Essa pode até ser uma solução preferível, pois permitiria muita flexibilidade para os usuários do *TrustChain*. Um usuário poderia, por exemplo, criar uma entrada confidencial que não inclua nada além do *hash* e da data/hora do documento, enquanto outro poderia usar uma ontologia mais complexa para seus documentos, o que os tornaria facilmente identificáveis por qualquer pessoa e adequados para indexação. A criação dessas ontologias provavelmente seguiria os padrões arquivísticos existentes.

Em segundo lugar, alguns críticos não viram a necessidade de um sistema desse tipo ou o consideraram uma complicação excessiva em relação aos esquemas de carimbo de tempo (*timestamping*) já existentes. A razão para o desenvolvimento do *TrustChain* foi preservar as informações de certificado (ou, pelo menos, informações sobre sua validade em determinado momento). De acordo com os pesquisadores da equipe TRUSTER, nenhum dos serviços de carimbo do tempo existentes atende a esse requisito. É claro que a implementação bem-sucedida do sistema *TrustChain* exige uma infraestrutura significativa, instituições participantes dispostas e, ainda, mais desenvolvimento, enquanto os serviços de *timestamping* são padronizados e comercialmente disponíveis neste momento. Entretanto, na visão dos pesquisadores da equipe, o *TrustChain* é uma solução melhor. A TRUSTER VIP Solution "*TrustChain*" demonstra que tal sistema é viável e que não é necessário re-assinar (ou aplicar novo carimbo de tempo) periodicamente os registros.

## 9. Conclusões

Uma sugestão para aumentar a segurança do *TrustChain* é adicionar a cada bloco um carimbo de tempo qualificado de terceiros. Embora isso complique ainda mais o sistema, é uma boa sugestão e, realmente, tornaria a blockchain mais segura. O modelo atual não considerou em detalhe seus próprios carimbos de tempo. Neste momento, supõe-se simplesmente que os nós que criam blocos e votos usam seus próprios horários internos de servidor. Essa não é uma boa solução e é certamente insuficiente do ponto de vista de segurança, pois deixa um vetor de ataque claro e possivelmente fácil de explorar. A dependência de carimbo de tempo, de relógios externos e de relógios internos é algo que será abordado em futuras pesquisas e no desenvolvimento do modelo.

Outra linha de pesquisa em andamento é a implementação de um esquema de chave transitória (*transient-key*) no *TrustChain*, seja como um recurso incorporado ou com base em um serviço externo. Uma chave transitória é uma variação do esquema PKI usual, na qual as chaves são emitidas por um período muito curto e estão vinculadas a um determinado intervalo de tempo em vez de a uma pessoa ou instituição. A vida útil de uma chave em tal sistema geralmente é limitada a alguns minutos, e uma lista com todas as chaves de intervalo anteriores é publicada e mantida por várias fontes publicamente disponíveis. Esse tipo de (terceiro) carimbo de tempo poderia ser adicionado a cada bloco como uma fonte de tempo externa confiável, atendendo aos requisitos mencionados anteriormente. Alternativamente, um esquema de chave transitória poderia ser incorporado ao próprio *TrustChain*. Um esquema de chave transitória é patenteado (Doyle, 2002), e isso pode ser um grande obstáculo para implementar tal sistema diretamente, mas ainda assim poderia ser utilizado como um carimbo de tempo externo caso a equipe considere essa solução preferível a um esquema baseado em encadeamento de blocos.

Uma possível evolução do sistema *TrustChain*, conforme sugerido pela Enigio Time – parceira desta pesquisa, é também armazenar os intervalos de validade dos certificados (e suas cadeias) em vez das informações de validade da assinatura digital. Se os períodos de validade dos certificados forem armazenados em uma estrutura de dados imutável, como uma blockchain, também seria possível confirmar que documentos que foram carimbados em data anterior à expiração do certificado de sua assinatura possuíam um certificado válido e, portanto, uma assinatura válida naquele momento. Isso poderia oferecer prova de sua autenticidade, além de garantir a integridade de dados por meio do seu carimbo de tempo ainda válido. Em longo prazo, uma combinação oficial de tal *TrustChain* com a infraestrutura de PKI poderia possivelmente eliminar o problema de certificados que expiram e beneficiar uma tecnologia consolidada como a PKI em combinação com a nova tecnologia de blockchain. Uma estrutura de dados e um sistema de votação semelhantes aos já apresentados poderiam ser adequados para armazenar essas informações também. A vantagem de tal sistema é que assinaturas já expiradas ainda podem ser controladas se possuírem um carimbo de tempo válido da época em que foram assinadas. Neste momento, ambas as variações estão sendo desenvolvidas e deverão funcionar de forma independente. Os títulos de trabalho das duas variantes são: *TrustChain-H* (preserva *hashes*) – a proposta original detalhada neste relatório – e *TrustChain-C* (preserva certificados) para a nova proposta de sistema que ainda será desenvolvida.

## 10. Produtos

Estudo de caso 1 – registros de fundo de aposentadoria assinados digitalmente

Estudo de caso 2 – registros de impostos eletrônicos assinados digitalmente

Estudo de caso 3 – registros médicos assinados digitalmente, contratos de aquisição e fornecedores, decisões políticas oficiais e atas de reuniões

Bibliografia sobre blockchain

Terminologia de blockchain – na base de dados de terminologia do InterPARES Trust

## 11. Lista de figuras e tabelas

### Lista de figuras



### Lista de tabelas

## 12. Referências

American National Standards Institute. (2016). Retrieved from ANSI X9.95-2016 Financial Services - Trusted Time Stamp Management And Security: https://infostore.saiglobal.com/en-gb/Standards/ANSI-X9-95-2016-1894464/

Atzori, M. (2016). *Blockchain Technology and Decentralized Governance:* Is the State Still Necessary? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

Blanchette, J.-F. (2006). The Digital Signature Dilemma: To Preserve or Not to Preserve. *Annales des Télécommunications*, 61(7-8), 908-923.

Boucher, P. (2016, September 29). *What if blockchain technology revolutionised voting?* Retrieved from http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA%282016%29581918_EN.pdf

Bradbury, D. (2014). *coindesk*. Retrieved from How Block Chain Technology Could Usher in Digital Democracy: https://www.coindesk.com/block-chain-technology-digital-democracy/

Bralić, V., Kuleš, M., & Stančić, H. (2017). A model for long-term preservation of digital signature validity: TrustChain. In I. Atanassova, W. Zaghouani, B. Kragić, K. Aas, H. Stančić, & S. Seljan (Ed.), *INFuture 2017: Integrating ICT in Society*, (pp. 89-113). Zagreb.

Chaum, D. (n.d.). Random-Sample Voting. Retrieved from https://rsvoting.org/whitepaper/white_paper.pdf

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). Retrieved from RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: https://tools.ietf.org/html/rfc5280

Croatian parliment. (2002). *Narodne Novine*. Retrieved from Electronic signature law (NN 10/2002): https://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html

Croatian Parliment. (2002). Narodne Novine. Retrieved from Electronic signature Act (NN 10/2002): https://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html

(2015). *Data Dictionary for Preservation Metadata:* PREMIS version 3.0.

Doyle, M. D. (2002). *Patent No. United States Patent 6381696*.

Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Frankfurt am Main: Apress.

Drummond, K. (2010). *Pentagon turns to brain implants to repair damaged minds*. Retrieved from Wired: https://www.wired.com/2010/05/pentagon-turns-to-brain-implants-to-repair-damaged-minds/

Dumortier, J., & Van den Eynde, S. (n.d.). Electronic Signatures and Trusted Archival Services. Retrieved 5 15, 2015, from http://www.expertisecentrumdavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf

ETSI. (2016). Retrieved from ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles: http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf

ETSI. (2016). ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation: http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.00_30/en_31910201v010100v.pdf

European Comission. (2016, February 29). Questions & Answers on Trust Services under eIDAS. Retrieved December 29, 2017, from https://ec.europa.eu/digital-single-market/en/news/questions-answers--trust-services-under-eidas

European Parliament. (2014). *eIDAS*. Retrieved from https://www.eid.as/home/

Hanson, R. (2000). Shall We Vote on Values, But Bet on Beliefs? Journal of Political Philosophy, 1-40.

Herceg, B., Brzica, H., & Stančić, H. (2015). Digitally signed records - friend or foe? in: Anderson, K., Duranti, L., Jaworski, R., Stančić, H., Seljan, S., and Mateljan, V. (eds), *INFuture 2015: e-Institutions - Openness, Accessibility and Preservation*, 147-150, Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb

Huminski, P. (2017). *The technology behind bitcoin could revolutionize these 8 industries in the next few years* . Retrieved 12 21, 2017, from Business Insider: http://www.businessinsider.com/8-applications-of-blockchain-2017-7

Ibrahimpašić, B., & Liđan, E. (2011). Digitalni potpis. *Osječki matematički list*, Vol.10 No.2, 139-148.

International Organization for Standardization. (2009). Retrieved from ISO/IEC 18014-3:2009 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens: https://www.iso.org/standard/50457.html

International Organization for Standardization. (2012). Retrieved from ISO 14721:2012 Space data and information transfer systems – Open archival information system (OAIS) – Reference model: https://www.iso.org/standard/57284.html

International Organization for Standardization. (2012). Retrieved 5 10, 2016, from ISO 16363:2012 Space data and information transfer systems – Audit and certification of trustworthy digital repositories: https://www.iso.org/standard/56510.html

International Organization for Standardization. (2012). Retrieved from ISO 16363:2012 Space data and information transfer systems -- Audit and certification of trustworthy digital repositories: https://www.iso.org/standard/56510.html

International Organization for Standardization. (2016). Retrieved from ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles: https://www.iso.org/standard/62542.html

InterPARES Trust Terminology Database. (n.d). Retrieved December 28, 2017, from http://arstweb.clayton.edu/interlex/en/term.php?term=trustworthiness

Katulić, T. (2011). Razvoj pravne regulacije elektroničkog potpisa, elektroničkog certifikata i elektroničke isprave u hrvatskom i poredbenom pravu. *Zbornik Pravnog fakulteta u Zagrebu*, Vol. 61, No. 4, 1343-1344.

Lemieux, V. L., & Sporny, M. (2017). Preserving the Archival Bond in Distributed Ledgers: A Data Model and Syntax. *Proceedings of the 26th International Conference on World Wide Web Companion*, (pp. 1437-1443).

Merkle, R. C. (1980). Protocols for public key cryptosystems. *IEEE Symposium on Security and Privacy*, 122, pp. 122-134.

Mihaljević, M., Mihaljević, M., & Stančić, H. (2015). *Archival science dictionary. English-Croatian, Croatian--English*. Zagreb: FF Press.

Miroslav Krleža Institute of Lexicography. (2017). *Hrvatska encikolpedija*. Retrieved from digitalizacija: http://www.enciklopedija.hr/natuknica.aspx?id=68025

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 11 21, 2015, from https://bitcoin.org/bitcoin.pdf

National Institute of Standards and Technology. (1999). Retrieved from Data Encryption Standard (DES): https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

National Institute of Standards and Technology. (2012). Retrieved from Digital Signature Standard (DSS): http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Nayuki. (2016, 1 4). Forcing a file's CRC to any value. Retrieved 105, 2017, from https://www.nayuki.io/page/forcing-a-files-crc-to-any-value

Rockwell, M. (n.d.). Retrieved from BitCongress - Process For Blockchain Voting & Law: http://bitcongress.org/BitCongress_Whitepaper.pdf

Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., & Adams, C. (2013). Retrieved from RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP: https://tools.ietf.org/html/rfc6960

## 13. Apêndice 1 – Modelo de Preservação TRUSTER (EU31) – Questionário de Estudo de Caso

Este questionário foi desenvolvido e utilizado para tornar os resultados dos estudos de caso comparáveis. Ele foi usado nos estudos de caso 1 e 2. Está dividido em 11 seções com as respectivas perguntas.

---

QUESTIONÁRIO

**Os registros em questão são:**

---

**Entrevistado:**

**Data da entrevista:**

**Nota importante**

---

---

As respostas às perguntas a seguir devem ser tratadas como confidenciais (se aplicável, por favor, indique):

---

---

**1. Número de documentos com certificados expirados**

**P:** Qual é o número de documentos com certificados expirados que estão sendo armazenados? É necessário saber para entender o volume de dados envolvidos.

**R:**

---

**2. Número de solicitações desses documentos com certificados expirados**

**P:** Quantas solicitações foram feitas para esses documentos? Isso pode nos ajudar a decidir quais documentos são mais importantes.

**R:**

**P:** Você está lidando com documentos acessíveis aos usuários?

**R:**

---

**3. Importância dos documentos**

**P:** Assim como na pergunta anterior, alguns documentos são mais importantes? Algum deles deve ter prioridade maior para preservação/migração etc.?

**R:**

---

**4. Idade dos documentos**

**P:** Quanto tempo se passou desde que os certificados dos documentos expiraram e qual o efeito disso na possível recertificação?

**R:**

---

**5. Intervalo de tempo dos documentos (quanto tempo desde a expiração dos certificados)**

**P:** Quanto tempo se passou desde que os certificados de determinados documentos expiraram? Consideramos isso relevante, pois um intervalo maior significa mais tempo para acesso não autorizado.

**R:**

---

**6. Forma de armazenamento e formatos dos documentos**

**P:** Você pode fornecer informações sobre como os documentos foram armazenados e em quais formatos? Que tecnologia foi usada e quão desatualizada ela está hoje? Isso é importante para encontrar uma solução para os certificados expirados.

**R:**

---

**7. Processo de aquisição dos documentos**

**P:** Como os documentos foram adquiridos e qual foi o processo de ingestão? Isso nos dará mais informações sobre como os documentos foram mantidos e as possibilidades de renovação dos certificados.

**R:**

---

**8. Gestão dos arquivos com assinaturas digitais expiradas**

**P:** Quem tem acesso aos documentos? Quem os gerencia? Como isso afeta a confiabilidade desses documentos? Como isso afeta a possível recertificação?

**R:**

---

**9. Status legal das assinaturas expiradas**

**P:** Quais critérios as assinaturas expiradas devem atender para serem consideradas legalmente válidas? Quem decide isso?

**R:**

---

**10. Uso empresarial**

**P:** Os registros problemáticos são realmente usados para fins empresariais? Se não, por que são mantidos e quais partes estão interessadas?

**R:**

**P:** Esses registros são relevantes para disputas de alto valor atuais ou previsíveis e processos judiciais?

**R:**

---

**11. Preservação de longo prazo**

**P:** Você investigou as seguintes opções como solução para problemas atuais ou futuros de preservação de longo prazo? Se sim, são viáveis?

**R:**

a. Revalidação de assinaturas históricas usando software/hardware especial e/ou serviços de terceiros
Não / Sim > É viável? Sim / Não

b. Reassinatura dos registros antes da expiração das assinaturas

Não / Sim > É viável? Sim / Não

c. Uso de serviços de e-notariado

Não / Sim > É viável? Sim / Não

d. Uso de serviços de carimbo do tempo e arquivamento digital de terceiros confiáveis

Não / Sim > É viável? Sim / Não

e. Blockchain

Não / Sim > É viável? Sim / Não

f. Eliminação dos registros problemáticos (alterando requisitos legais, se necessário)

Não / Sim > É viável? Sim / Não

g. Validação dos registros no momento da captura em sistema arquivístico confiável, confiando posteriormente no sistema para garantir integridade, usabilidade e autenticidade ao longo do tempo

Não / Sim > É viável? Sim / Não

h. Criação de sistema de gestão de registros que assegure evidências circunstanciais sólidas de sua integridade e autenticidade

Não / Sim > É viável? Sim / Não

---

i. Outra (especifique)

**P:** Você avaliou o custo da preservação (em vários cenários) versus os riscos (como multas por não conformidade, danos pagos em processos judiciais etc.)?

**R:**

**P:** Quão certo você está de que o problema, uma vez resolvido, não se repetirá no futuro?

**R:**

a. Incerto

b. Pouco certo

c. Razoavelmente certo

d. Certo

e. Não sabe

Cariniana

Rede Brasileira de Serviços de Preservação Digital