CEFET/RJ
campus Nova Friburgo

DIGITAL LEFT MANAGEMENT: UMA PROPOSTA

Henrique Júnior de Souza Oliveira

Monografia apresentada ao Curso de Graduação em Sistemas de Informação, do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ Campus Nova Friburgo, como parte dos requisitos necessários à obtenção do certificado de Bacharel em Sistemas de Informação.

Orientador(a): Nilson Mori Lazarin

Rio de Janeiro
Janeiro de 2021

DIGITAL LEFT MANAGEMENT: UMA PROPOSTA

Monografia apresentada ao Curso de Graduação em Sistemas de Informação, do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ Campus Nova Friburgo, como parte dos requisitos necessários à obtenção do certificado de Bacharel em Sistemas de Informação.

Henrique Júnior de Souza Oliveira

Banca Examinadora:

NILSON MORI LAZARIN:72809353115

Assinado de forma digital por NILSON MORI LAZARIN:72809353115
DN: cn=NILSON MORI LAZARIN:72809353115, ou=CEFET-RJ - Centro Fed. Educ. Tecnol. Celso S. Fonseca, o=ICPEdu, c=BR
Dados: 2021.02.11 14:43:24 -03'00'

Presidente, Professor Me. Nilson Mori Lazarin (CEFET/RJ) (orientador)

BRUNO POLICARPO TOLEDO FREITAS:00484594028

Assinado de forma digital por BRUNO POLICARPO TOLEDO FREITAS:00484594028
Dados: 2021.02.11 15:04:13 -03'00'

Professor Me. Bruno Policarpo Toledo Freitas (CEFET/RJ)

LUIS CLAUDIO BATISTA DA SILVA:07180635707

Assinado de forma digital por LUIS CLAUDIO BATISTA DA SILVA:07180635707
Dados: 2021.02.11 14:48:22 -03'00'

Professor Dr. Luis Claudio Batista da Silva (CEFET/RJ)

CARLOS EDUARDO PANTOJA:05634242738

Assinado de forma digital por CARLOS EDUARDO PANTOJA:05634242738
DN: cn=CARLOS EDUARDO PANTOJA:05634242738, ou=CEFET-RJ - Centro Fed. Educ. Tecnol. Celso S. Fonseca, o=ICPEdu, c=BR
Dados: 2021.02.11 21:16:15 -03'00'

Professor Dr. Carlos Eduardo Pantoja (CEFET/RJ)

Rio de Janeiro
Janeiro de 2021

Ficha catalográfica elaborada pela Biblioteca Central do CEFET/RJ

RESUMO

Digital Left Management: Uma proposta

Contratos Inteligentes se apresentam com grande potencial de aplicação em sistemas de DRM (*Digital Rights Management* - Gerenciamento de Direitos Digitais) de modo a garantir os direitos de ativos digitais sem prejudicar a liberdade do usuário, uma vez que os atuais sistemas têm se efetivado como mecanismos de controle e restrição, limitando a sensação de posse de consumidores de obras digitais. Este trabalho apresenta um modelo de gerenciamento de direitos sobre ativos digitais protegidos pelo direito autoral, através de Contratos Inteligentes, como possível solução ao desafio de garantir a liberdade de uso do usuário que o adquiriu sem ferir os direitos autorais. O modelo proposto busca alinhar a ideia de empréstimo e/ou venda de arquivos digitais ao conceito de gerenciamento automático de direitos digitais através do uso de Contratos Inteligentes.

Palavras-chave: Contrato Inteligente; Blockchain; DRM

ABSTRACT

Digital Left Management: A proposal

Smart Contracts present themselves with great potential for application in DRM (Digital Rights Management) systems in order to guarantee the rights of digital assets without jeopardizing the user's freedom, since the current systems have been implemented as control and restriction mechanisms, limiting the feeling of ownership of consumers of digital works. This work presents a model for managing rights over digital assets protected by copyright, through Smart Contracts, as a possible solution to the challenge of guaranteeing the freedom of use of the user who acquired it without harming copyright. The proposed model seeks to align the idea of borrowing and / or selling digital files with the concept of automatic digital rights management through the use of Smart Contract.

Keywords: Smart Contract; Blockchain; DRM

SUMÁRIO

1 - Introdução

Há alguns anos, as mídias físicas de CD e DVD, por exemplo, passaram por diversos problemas em relação à proteção dos direitos autorais. Isso porque essas mídias poderiam ser copiadas de qualquer computador e reproduzidas ou vendidas ilegalmente na sociedade [IANZEN et al. 2013]. Sendo assim, em 1996 foi criada a tecnologia DRM (*Digital Rights Management*) com o objetivo de proteger os direitos autorais do conteúdo dessas mídias e tentar conter o avanço da pirataria [OLIVEIRA 2019]. No entanto, o alto nível de restrição desta tecnologia imposta pelas empresas fez com que vários usuários compradores questionassem sobre seus direitos de uso e reprodução em diferentes dispositivos, pois não tinham a permissão de uso total daquilo que haviam adquirido e tomado como posse; fato este que, até os dias atuais, vem ocorrendo com os ativos digitais compartilhados pela internet [IANZEN et al., 2013; OLIVEIRA 2019].

1.1 – Problema

Diante de tantas inovações e facilidades de compartilhamento de arquivos digitais por meio da Internet, a gestão e a proteção desses ainda é um dos desafios da atualidade, pois à medida em que há o avanço da tecnologia de distribuição de conteúdos digitais crescem também a pirataria e a distribuição ilegal desses conteúdos [IANZEN et al. 2013]. Sendo assim, editoras e/ou autores têm optado obrigatoriamente por sistemas de Gerenciamento de Direitos Digitais (DRM), com o intuito de gerir e proteger suas obras no ambiente digital.

A gestão de ativos digitais se refere ao controle de permissão de acesso e leitura do conteúdo dado ao usuário final. Já a proteção se refere ao nível de segurança adotado para que o ativo digital não seja replicado indevidamente ou utilizado sem autorização. Consequentemente, com o maior nível de aceitabilidade de usuários/leitores no que diz respeito aos conteúdos digitais (como por exemplo, os livros digitais conhecidos como *E-books*) o mercado editorial vem enfrentando um sério problema em relação ao direito autoral [IANZEN et al. 2013]. Garantir os direitos autorais de uma obra distribuída digitalmente ainda tem sido uma tarefa complexa para editoras, distribuidoras ou autores [OLIVEIRA et al. 2019].

Sendo assim, sistemas de DRM têm sido adaptados e desenvolvidos com o

objetivo de abranger a proteção legal dos conteúdos distribuídos eletronicamente. Alguns *players* do mercado, como a Amazon com o Kindle, a Apple com o iBooks e a Google com o Play Livros investem em tecnologias de DRM próprios que disponibilizam o conteúdo apenas para quem possui permissão para consumí-lo [OLIVEIRA et al. 2019]. No entanto, esses sistemas não tratam o usuário final como o detentor, ou seja, como proprietário do conteúdo adquirido, mas sim, como um usuário que tem alguns direitos de uso sobre aquele conteúdo, o que vem sendo muito questionado no âmbito editorial [IANZEN et al. 2013].

1.2 – Motivação

Portanto, como as discussões sobre o uso das obras protegidas por direitos autorais ainda não foram resolvidas, as criações que empregam novas tecnologias como a Blockchain e os Contratos Inteligentes começam a ganhar a atenção das pesquisas e debates sobre o futuro digital e o direito autoral [OLIVEIRA 2019].

A tecnologia Blockchain, adotada e destacada pelas criptomoedas, tomou uma proporção ainda maior em relação a sua capacidade de realizar e armazenar transferências de conteúdos digitais de forma descentralizada, segura e confiável. Isso ocorreu devido ao surgimento dos Contratos Inteligentes, revelando possibilidades muito além do que apenas transacionar valores monetários digitais. Essas inovações prometem uma maior automatização na criação, no licenciamento e no controle do uso de ativos digitais, de maneira a moldar os comportamentos humanos a partir de diretrizes de design tecnológico. Além disso, as tecnologias Blockchain e Contrato Inteligente poderão ser direcionadas para reforçar a posição pela liberdade de informação, e, consequentemente, pela visão do direito de autor como um meio de difusão de cultura e conhecimento [LANA 2019].

Sendo assim, foi realizada uma pesquisa na cidade de Nova Friburgo-RJ sobre o nível de aceitação do modelo proposto; um formulário com perguntas e respostas (objetivas e dissertativas) com o intuito de compreender qual seria o público que mais utiliza e-books, qual o seu nível de satisfação sobre esse modelo digital atual, qual a preferência de leitura (livro físico ou digital) e o porquê da escolha, e qual seria o nível de aceitação do modelo de empréstimo entre usuários sobre o livro digital. Este formulário foi publicado nas redes sociais (principalmente, Whatsapp) no período compreendido entre os dias 26/05/2019 e 07/06/2019, obtendo 91 respostas de pessoas de diferentes faixas etárias e sexo (conforme gráficos no APÊNDICE A).

De acordo com a pesquisa, pode-se dizer que há uma gama de pessoas que ainda não estão satisfeitas com os livros digitais atuais, devido às suas limitações funcionais ou sensação de posse. Destas, 80% das pessoas que responderam sobre o livro digital (e-book) disseram que não havia a funcionalidade de empréstimo do livro para outra pessoa e que gostariam que tivesse essa funcionalidade nas plataformas e, cerca de 90% das pessoas acham que a ideia é muito boa.

1.3 – Contribuição

Portanto, este trabalho, cujo acrônimo "DLM" significa *Digital Left Management* em adesão à ideia de Copyleft[1], tem como objetivo apresentar uma proposta de gestão de direitos digitais que visa garantir tanto os direitos autorais aos detentores dos arquivos digitais, de forma transparente, confiável e segura, quanto garantir a liberdade e a flexibilidade de uso aos usuários de ativos digitais, podendo realizar empréstimos e/ou revendas desses arquivos através da Internet. Diferentemente de tecnologias convencionais de *Digital Rights Management* (DRM) que deturparam os propósitos de incentivo às criações e de propagação das obras na cultura, tendo se desdobrado em maiores privilégios aos detentores de direitos autorais [OLIVEIRA et al., 2019; OLIVEIRA, 2019; FUJIMURA et al., 2015].

1.4 – Estrutura do trabalho

No capítulo 2 é apresentada a Revisão Bibliográfica sobre alguns conceitos e tecnologias de estudo necessários para o entendimento do modelo proposto.

No capítulo 3 são abordadas 3 seções de trabalhos relacionados sobre gerenciamento de direitos digitais através da tecnologia Blockchain e uma proposta para empréstimo de arquivos digitais e, um comparativo entre esses trabalhos e o modelo proposto.

No capítulo 4 é apresentada a Proposta deste trabalho: Implementação e um Comparativo entre o modelo proposto e alguns DRMs existentes no mercado.

No capítulo 5 são feitas as considerações finais.

[1] https://www.gnu.org/licenses/copyleft.pt-br.html

2 - Revisão Bibliográfica

Para melhor compreensão do modelo proposto e das tecnologias que foram utilizadas, este capítulo aborda a referência bibliográfica de conceitos e técnicas relacionados ao modelo DRM, desde seu objetivo até a sua arquitetura de forma genérica, além de apresentar as tecnologias envolvidas no processo criptográfico dos ativos digitais como: o algoritmo simétrico, o algoritmo assimétrico e a função *hash*. Já para o gerenciamento e validações de permissões dos direitos digitais foram abordadas as tecnologias Blockchain e Contratos Inteligentes.

2.1 – *Digital Rights Management* (DRM)

O *Digital Rights Management* (DRM) foi formado a partir da ideia de Copyright, que é o direito exclusivo dado a um criador ou procurador de imprimir, publicar, representar, filmar ou gravar um material literário (artístico ou musical) e de autorizar os outros a fazer o mesmo. No entanto, até então, o Copyright subsistia apenas em obras de autorias originais em meios tangíveis de expressão, os quais poderiam ser reproduzidas ou de alguma forma comunicadas. Por exemplo: obras literárias, musicais, teatrais, arquitetônicas, gravações de áudio ou audiovisuais e etc [MORAES 2014].

No contexto do meio digital, pode-se dizer que o Digital Rights Management (DRM) são sistemas de gerenciamento de direitos digitais que aplicam restrições de cópia, distribuição ou acesso ao conteúdo digital, cujo objetivo é controlar o uso pós venda e prevenir o uso indevido de determinados arquivos eletrônicos. As técnicas de DRM têm por intuito direcionar os comportamentos dos usuários no consumo de bens virtuais aplicando três ações gerais: limitar, monitorar e direcionar [OLIVEIRA, 2019; OLIVEIRA et al., 2019; MORAES, 2014].

- **Limitação:** visa gerenciar o nível de permissão do usuário sobre um bem digital, como por exemplo, autorizando a leitura de uma obra, mas bloqueando a sua edição [OLIVEIRA, 2019; OLIVEIRA et al., 2019].
- **Monitoramento:** busca enviar relatórios automatizados acerca de atividades

do usuário no consumo daquele bem [OLIVEIRA, 2019; OLIVEIRA et al., 2019].

- **Direcionamento:** prevê o uso de protocolos para reforçar consequências contra um uso indesejado, tais como encerrar a execução de um programa como penalidade por detectar o uso não autorizado de uma mídia [OLIVEIRA, 2019; OLIVEIRA et al., 2019].

Esta capacidade de interferir na maneira como o produto é consumido, que tornou o DRM uma tecnologia controversa, uma vez que ela tange desde a produção até o consumo do mesmo, podendo armazenar informações dos usuários, rastrear seus hábitos e disseminar estas informações para terceiros; podendo infringir alguns direitos dos consumidores e até impossibilitar atividades completamente legais, como realizar cópias de backup de CDs ou DVDs que possuam a tecnologia [MORAES 2014].

Logo, observa-se que o principal objetivo do DRM é de preservar os interesses dos detentores do Copyright. A princípio, a intenção desse sistema era apenas controlar a cópia dos conteúdos digitais; mas, em sua segunda geração o DRM controlava não só a cópia desses conteúdos, mas também, a visualização, a impressão, a alteração e, até mesmo, os dispositivos nos quais o conteúdo seria utilizado [MORAES 2014].

Levando-se em conta a rápida evolução da internet e dos dispositivos de mídia (como o CD/DVD), é perceptível e compreensível a preocupação das grandes empresas (detentoras de Copyrights) em fazer valer seu direito num ambiente no qual é muito fácil copiar ou distribuir suas obras. Consequentemente, estas empresas se viram na necessidade de desenvolver uma tecnologia que pudesse impor as restrições de Copyright no ambiente digital [OLIVEIRA, 2019; OLIVEIRA et al., 2019; MORAES, 2014].

Sendo assim, percebe-se uma linha tênue entre a garantia dos direitos dos detentores do Copyright e a garantia do direito de uso do consumidor sobre o material adquirido. É exatamente esse o maior desafio do DRM: garantir os direitos de Copyright sem afetar a experiência do consumidor, funcionando da forma mais transparente possível [OLIVEIRA, 2019; OLIVEIRA, et al. 2019; MORAES, 2014].

Modelo DRM

O modelo da tecnologia DRM pode seguir diferentes abordagens, desde mais intrusivas até menos intrusivas e usando diferentes arquiteturas. Porém, apesar de ser um modelo flexível, a tecnologia conta com alguns requisitos e componentes básicos para o seu funcionamento [MORAES 2014]. Os pré-requisitos desejáveis, no qual, podem existir ou não nos sistemas atuais são:

1. **Usabilidade:** o sistema DRM deve garantir que é de fácil uso para todos os envolvidos no fluxo de distribuição, tanto para o consumidor final quanto para os detentores de Copyright e distribuidores de conteúdo [BECKER 2003].

2. **Confiabilidade:** trata do quanto os usuários envolvidos estão seguros de que o sistema irá se comportar da forma que foi planejada. Ou seja, para os detentores de Copyright, por exemplo, o sistema deverá garantir que o acesso a determinado conteúdo digital esteja disponível somente ao usuário que o adquiriu. Em contrapartida, o sistema deverá garantir que esse usuário final tenha acesso a esse conteúdo [BECKER 2003].

3. **Segurança:** é uma das características de maior preocupação quando se fala de DRM. Isso porque é muito difícil achar um sistema 100% seguro, pois o endurecimento da segurança traz consigo um custo bem alto, tanto financeiro quanto na diminuição da usabilidade do sistema. Seria completamente inviável, por exemplo, proteger um conteúdo com um valor X em um sistema de segurança que custa 2X. Sendo assim, o nível de segurança deve se adequar a necessidade do conteúdo. Além disso, a robustez do sistema também é um dos grandes aspectos de segurança, na qual, se trata do nível de dificuldade de se remover os dispositivos de segurança sobre o conteúdo digital, permitindo que mesmo que sua segurança seja quebrada ele possa ser reconhecido depois como uma cópia ilícita [BECKER, 2003; MORAES, 2014].

4. **Flexibilidade:** a distribuição de conteúdo online é relativamente um método novo e que, portanto, existem diversas formas de se implementar. Sendo assim, o sistema DRM tem que ser flexível o suficiente para que consiga

trabalhar com essas novas ideias e conceitos de distribuição de conteúdo [BECKER 2003].

5. **Capacidade de implementação:** é um item de especial interesse aos fabricantes de dispositivos, pois diz respeito aos recursos necessários para suportar um sistema DRM. Os algoritmos a serem escolhidos, por exemplo, tendem a ser definidos de acordo com o tipo de dispositivo no qual o conteúdo será distribuído. Um leitor de e-books, por exemplo, será trabalhado com algoritmos que levem em consideração sua menor memória e poder de processamento em relação a um computador. Portanto, as capacidades dos dispositivos podem servir como severos meios de restrição das capacidades técnicas do DRM, mostrando a necessidade de se analisar alguns itens como: capacidade de memória, processador, conexão e até mesmo alguns requisitos de hardware ou software, como o sistema operacional [BECKER, 2003; MORAES, 2014].

6. **Interoperabilidade:** capacidade dos sistemas DRM de lidarem com outros sistemas. Ao adquirir um e-book protegido por DRM, por exemplo, o usuário precisa se preocupar se esse conteúdo será lido corretamente pelos leitores de e-books que possui em seu computador e/ou tablet. Sendo assim, dispositivos, serviços e conteúdos devem ser suficientemente interoperáveis para que o conteúdo possa ser distribuído eficientemente. Já houveram várias tentativas de distribuição de música de forma protegida, porém, os dispositivos / softwares capazes de reproduzir essas músicas eram relativamente restritos e as diferentes distribuidoras possuíam tecnologias DRM incompatíveis. Sendo assim, era impossível a reprodução de vários conteúdos diferentes pelo mesmo dispositivo, já que cada tecnologia poderia estar associada a um software diferente [BECKER, 2003; MORAES, 2014].

Não existe uma arquitetura padrão para o DRM, cada desenvolvedor pode criar a sua própria arquitetura. Porém, toda arquitetura segue um modelo bastante semelhante, conforme a Figura 1 [MORAES 2014]. Esta arquitetura do sistema DRM genérico está dividida em 3 partes:

1. **Definição de Itens:** se refere ao processo de criação e gerenciamento da propriedade intelectual de forma a simplificar sua comercialização. Sendo assim, é responsável pela validação, criação e fluxo de direitos.
2. **Gerenciamento de Conteúdo:** trata do processo de gerenciar metadados como utilização, pagamentos e etc. além de permitir a comercialização de conteúdo. Sendo assim, permite o acesso a dados e metadados no repositório e permite emissões de licenças para aqueles que estão autorizados a acessar o conteúdo.
3. **Uso do Conteúdo:** se refere a utilização do conteúdo pós-venda, aplicando tanto o gerenciamento das permissões quanto o monitoramento de uso do conteúdo.

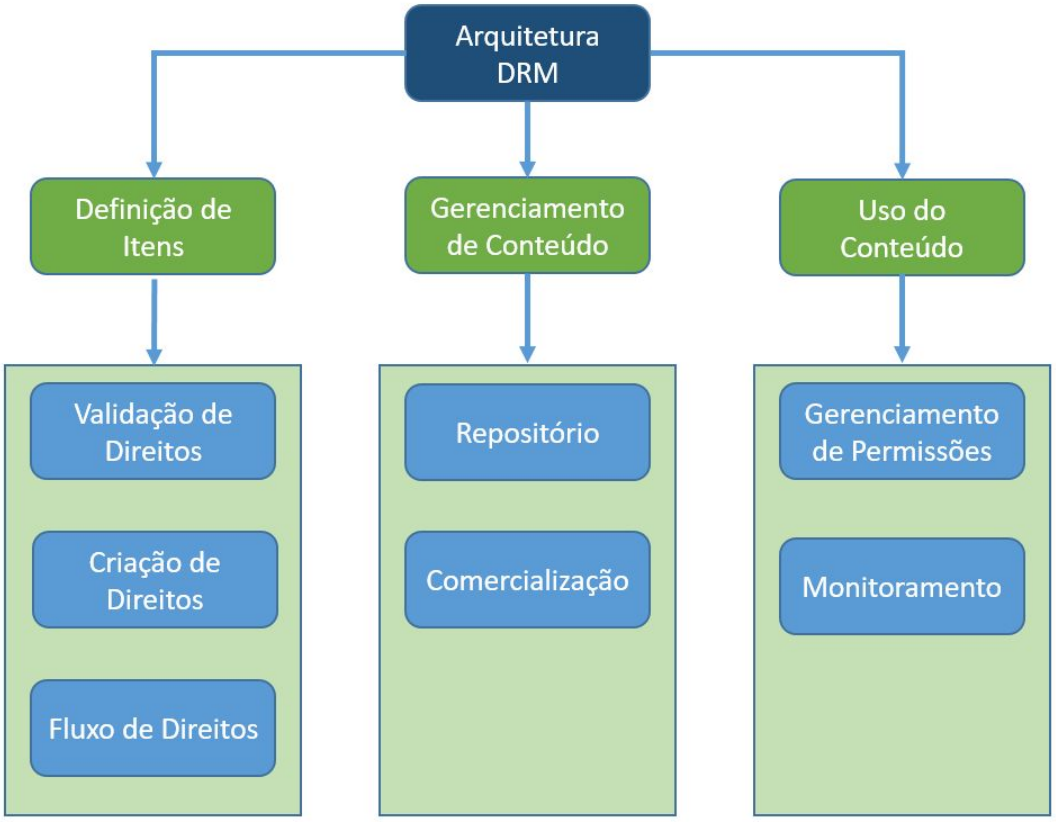


Figura 1. Arquitetura de um sistema DRM genérico - Adaptado de [MORAES 2014]

2.2 – Criptografia

O algoritmo criptográfico consiste basicamente em “embaralhar” e “esconder” informações sigilosas como, por exemplo, o conteúdo de um arquivo ou uma chave necessária para abrir o mesmo, de forma que torne o conteúdo ininteligível para aqueles que não possuem a chave do código necessária para decifrá-lo. Portanto, o processo criptográfico pode ser definido como “*o ato ou a arte de escrever em caracteres secretos*”, ou ainda como “*codificar dados de modo que só possam ser decodificados por indivíduos específicos*” [KIM, 2014; MORAES, 2014; TERADA, 2008].

Cifrar e decifrar dados é um criptossistema que normalmente envolve um algoritmo, conhecido como cifra, e combina os dados originais, conhecidos como texto claro ou texto simples, com uma ou mais chaves. A chave é uma sequência de caracteres alfanuméricos que deverá ser conhecida pelo emissor (para cifrar) e pelo destinatário da mensagem cifrada (para decifrar), de modo a descobrir o texto original [Kim, 2014; TANENBAUM, 2003].

A segurança de um criptossistema depende normalmente do segredo das chaves (seu tamanho é muito importante) e não só da cifra. Quanto maior for a chave, mais alto será o fator de trabalho para “descobrirem” a chave por exaustão de tentativas. O fator de trabalho para decodificar o sistema através de uma exaustiva pesquisa no espaço da chave é exponencial em relação ao tamanho da chave. Logo, o sigilo é decorrente da presença de um algoritmo forte e de uma chave longa. Segundo o Princípio de Kerckhoff: “*Todos os algoritmos devem ser públicos; apenas as chaves são secretas*” [TANENBAUM 2003].

O grau da “força” criptográfica é uma função de vários componentes. Por exemplo: o algoritmo e tamanhos de chave são dois dos componentes mais importantes que ajudam a determinar o quão difícil é quebrar o sistema de criptografia que está sendo usado [GALLO e HANCOCK 2003].

Um criptossistema forte tem uma gama de chaves possíveis, o que inviabiliza testar todas elas em um possível ataque de força bruta, por exemplo. Além disso, o criptossistema deve produzir texto cifrado de modo aleatório a cada teste estatístico-padrão e, portanto, mudando a chave, a saída da função criptográfica

também muda, mesmo que o texto claro se mantenha [KIM 2014].

Basicamente, a criptografia oculta informações de modo a garantir a segurança dessas informações. Porém, essa não é a única forma de proteger informações, tratando-se de um conjunto de ferramentas para segurança de TI.

A criptografia cumpre três objetivos de segurança [KIM, 2014; LAZARIN, 2012]:

1. **Confidencialidade:** mantém a informação secreta a todos, exceto ao pessoal autorizado. A criptografia torna a informação ininteligível a qualquer pessoa que não conheça a cifra de encriptação e a chave apropriada.
2. **Integridade:** garante que ninguém, nem mesmo o emissor, altere a informação após transmiti-la. Se uma mensagem não for decifrada apropriadamente, por exemplo, significa que alguém ou algo provavelmente mudou o texto cifrado no caminho.
3. **Autenticação:** confirma a identidade digital de uma entidade, que pode ser um emissor, o computador do emissor, algum dispositivo ou alguma informação; garantindo que remetente e destinatário sejam quem afirmam ser, impedindo que uma das partes negue uma declaração ou ação prévia. Ou seja, com a criptografia, pode-se provar matematicamente que determinada parte originou uma mensagem específica em uma hora específica de modo que seja irrefutável. Logo, a cifragem faz mais do que apenas manter secretas as mensagens; ela pode validar a identidade do emissor.

Apesar da cifragem de dados prover um grau de segurança relativamente alto, isso não significa necessariamente que os dados cifrados são seguros. Nada dura para sempre, e isso inclui a criptografia. Há sempre um jeito de explorar uma fraqueza em um algoritmo ou estrutura de chave na criptografia, mas isso pode ser muito difícil de fazer [GALLO e HANCOCK 2003].

A questão real com o uso de criptografia também é econômica: os dados são suficientemente valiosos para justificar o poder computacional e a energia pessoal necessários para decifrar o que quer que seja que está sendo transmitido na rede? Em caso de afirmativo, então ainda pode ser um alvo. Em caso negativo, esquemas de criptografia menos complexos podem ser mais que suficientes para a necessidade de segurança [GALLO e HANCOCK 2003].

Alguns algoritmos de cifragem não possuem algoritmos para decifrar, portanto, são chamados de algoritmos unidirecionais. Sendo assim, a saída de um algoritmo

unidirecional é o que se chama de *hash* [KIM 2014].

As cifras de encriptação podem pertencer a duas categorias: [KIM, 2014; GALLO e HANCOCK, 2003]

- Aquelas que usam a mesma chave para cifrar e decifrar, chamadas de *chaves simétricas;*
- Aquelas que usam chaves diferentes para cifrar e decifrar, chamadas de *chaves assimétricas.*

2.2.1 – Algoritmo Simétrico

Cifras de chave simétrica utilizam a mesma chave para cifrar e decifrar. Como resultado elas exigem que as duas partes primeiro troquem chaves para se comunicarem representando uma limitação básica para esses criptossistemas. Antes que seja enviada uma mensagem para outra parte é preciso fazer a troca das chaves com segurança [TANENBAUM 2003]. Diffie e Hellman explicaram: "*O custo e o atraso impostos por esse problema de distribuição de chaves são uma importante barreira para a transferência de comunicações de empresas para grandes redes de teleprocessamento*" [KIM 2014]. No entanto, um sistema simétrico é mais rápido e mais simples de se implementar, se comparado ao sistema assimétrico [LAZARIN 2012].

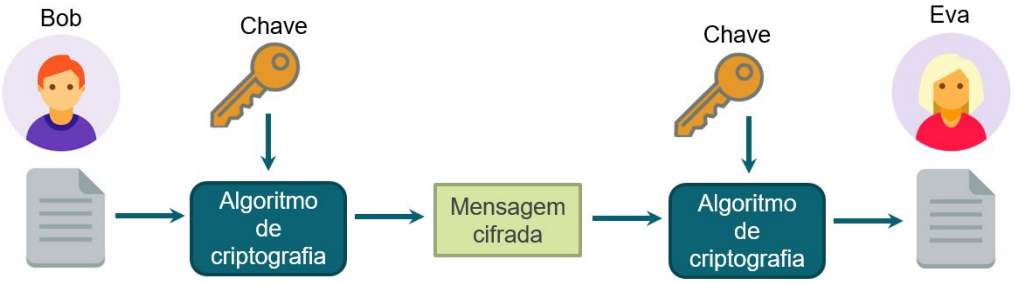


Figura 2. Criptografia Simétrica

Conforme a figura 2, o conteúdo enviado por Bob é cifrado com uma chave. A mensagem cifrada que chega até Eva é decifrada com a mesma chave que Bob utilizou para cifrar o conteúdo. Ou seja, tanto Bob quanto Eva têm acesso à mesma chave que é usada tanto para cifrar quanto para decifrar o conteúdo do arquivo.

O *Advanced Encryption Standard* (AES) especifica um algoritmo criptográfico

aprovado pelo FIPS 197 (*Federal Information Processing Standards Publication*) que pode ser usado para proteger dados digitais. O algoritmo AES é uma cifra de bloco simétrico que pode cifrar e decifrar informações. A criptografia converte os dados em uma forma ininteligível chamada de texto cifrado. Decifrando o texto cifrado, os dados são convertidos de volta em sua forma original, chamados de texto simples. Além disso, o algoritmo AES é capaz de usar chaves criptográficas de 128, 192 e 256 bits para cifrar e decifrar dados em blocos de 128 bits [NIST FIPS-197].

2.2.2 – Algoritmo Assimétrico

Este algoritmo é um método de encriptação amplamente aceito e implementado que requer duas chaves para cada usuário, uma pública e outra privada. Cada chave pública de usuário está disponível para qualquer um, enquanto a chave privada é secreta e conhecida apenas pelo usuário. Uma mensagem codificada com a chave pública é decodificada com a chave privada e vice-versa, conforme figura 3 [GALLO e HANCOCK, 2003; LAZARIN, 2012].

O RSA é um algoritmo de encriptação de chave pública, ou chaves assimétricas, e seu nome vem das iniciais do sobrenome dos autores: Ronald River, Adi Shamir e Len Adleman. O RSA é um algoritmo matemático que tem suas raízes em um ramo da matemática pura conhecido como Teoria dos Números. O esquema básico do algoritmo envolve conceitos elementares desta Teoria, tais como: números primos, máximo divisor comum (MDC) e sistemas modulares [GALLO e HANCOCK 2003].

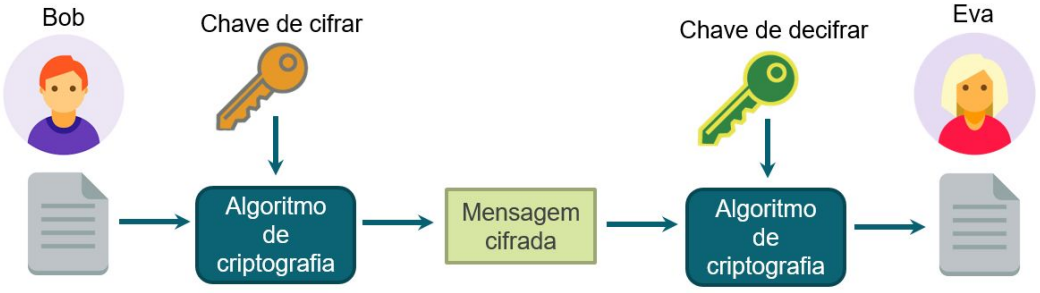


Figura 3. Criptografia Assimétrica

A menor velocidade na cifração e decifração, em relação aos sistemas simétricos, faz com que ambos os sistemas sejam comumente usados em uma comunicação, de forma que, o sistema assimétrico é utilizado para transmitir a chave que será utilizada pelo sistema simétrico [LAZARIN 2012].

Cifras de chaves assimétrica possuem quatro propriedades fundamentais: [KIM 2014]

- **Existem dois algoritmos associados e inversos -** Isso significa que existe um algoritmo para cifrar e outro para decifrar.
- **Cada um destes dois algoritmos é fácil de calcular -** Esta abordagem pode ser utilizada em software computacional sem muita dificuldade. Como resultado, ela se torna prática para comunicações digitais seguras.
- **É computacionalmente inviável derivar o segundo algoritmo se souber o primeiro -** É possível publicar uma chave amplamente para qualquer pessoa usar sem comprometer o conteúdo da chave associada a ela. São pares de uma chave pública e sua chave privativa associada ou um par de chaves pública-privada.
- **Dada alguma entrada aleatória, pode-se gerar pares de chaves associadas e inversas -** Qualquer parte pode criar pares de chaves pública-privada, manter uma chave privada e publicar a outra em um diretório para que qualquer correspondente utilize. Como a chave privativa é secreta e nunca é transmitida, um “curioso” não poderá descobrir esse valor.

2.2.3 – *Hash*

Funções de *Hash* ajudam a detectar falsificações, calculam uma soma de verificação de uma mensagem e depois a combinam com uma função criptográfica, de modo que o resultado seja inviolável. Porém, vale destacar que essas somas de verificação não garantem sigilo, mas sim, integridade; pois essas somas são muito simples e possível de aparecerem corretamente em uma mensagem trocada. *Hashes* normalmente são de um tamanho fixo conhecido, com base no algoritmo utilizado e o

resultado é um valor de *hash* [KIM 2014].

Um *hash* é uma soma de verificação projetada de modo que seja muito difícil forjar uma mensagem que resulte no mesmo *hash* de uma mensagem legítima; atuando como uma impressão digital dos dados. Ou seja, os *hashes* podem ser disponibilizados como referência para que os destinatários possam verificar a integridade da informação [CHAGAS, 2019; KIM, 2014; LANA, 2019].

O professor Ronald Rivest, do MIT (o R em RSA), desenvolveu o algoritmo de resumo de mensagem MD5. A [RFC 1321, 1992] contém especificações para o algoritmo, que toma uma entrada de qualquer tamanho arbitrário e gera um resumo de mensagem de 128 bits, cuja correspondência é computacionalmente inviável por outra entrada. Esse resumo de mensagem é associado exclusivamente à sua origem. É importante destacar que o MD5 não garante autenticidade, mas sim, integridade; provando que o arquivo não foi mudado desde o cálculo do *hash* [KIM 2014].

A [FIPS 180-1] (*Federal Information Processing Standard Publication* 180-1) define o Algoritmo de Hash Seguro (SHA-1 --- *Secure Hash Algorithm*), SHA-1 produz um *hash* de 160 bits a partir de uma mensagem de qualquer tamanho arbitrário. Assim como o MD5, ele cria uma impressão digital exclusiva de um arquivo computacionalmente inviável de reproduzir [KIM, 2014; FIPS 180-1].

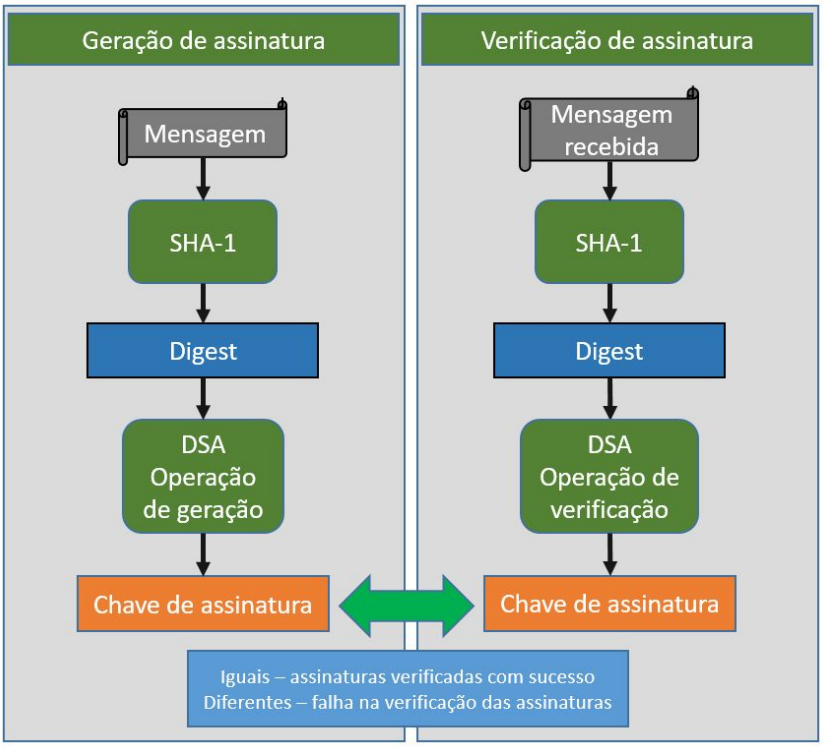


Figura 4. Usando o SHA-1 com o DSA - Adaptado de [FIPS 180-1]

De acordo com [FIPS 180-1], na Figura 4, o SHA-1 especifica um algoritmo de *hash* seguro para calcular uma representação condensada de uma mensagem ou arquivo de dados. Quando uma mensagem de qualquer comprimento menor que 2^{64} é entrada, o SHA-1 produz uma saída de 160 bits chamada de Digest. Este pode ser, então, inserido no *Digital Signature Algorithm* (DSA) ou Algoritmo de Assinatura Digital, que gera ou verifica a assinatura da mensagem. O Digest é assinado ao invés da mensagem original porque geralmente melhora a eficiência do processo, pois o Digest geralmente é muito menor do que o tamanho da mensagem original.

2.3 – Blockchain

A Blockchain é uma tecnologia que surgiu em 2008, por Satoshi Nakamoto, com o objetivo de registrar as transações da criptomoeda Bitcoin sem a necessidade de terceiros para resolver os problemas de *gastos duplos*[2]. Sendo assim, a Blockchain também é conhecida como um "livro distribuído", na qual envolve vários participantes na rede que devem chegar a um consenso sobre um conjunto de dados. Os sistemas Blockchain são desenvolvidos em diferentes modelos de confiança com diferentes protocolos de consensos e foi projetada para manter características típicas de uma cadeia, com continuidade e confiabilidade durante todo o processo, o que leva a integridade das informações [ALECRIM, 2019; CHAGAS, 2019].

A continuidade nesta tecnologia é definida como blocos, como se fossem elos de uma cadeia que se sucedem em uma sequência lógica, formando a chamada Blockchain. Nesse sentido, a confiabilidade é definida como a impossibilidade de substituir ou remover um bloco desta cadeia [ALECRIM 2019].

A ideia básica por trás dessa tecnologia é que ela permite que atores façam transações de ativos digitais dentro de um sistema, utilizando-se da arquitetura *peer-to-peer* (P2P) para que transações sejam feitas de forma descentralizada e sejam armazenadas de forma distribuída em toda a rede. Esta arquitetura consiste em uma cadeia de blocos ordenados de forma sequencial e cronológica, por meio da qual o

[2] Gastos duplos de Bitcoin (BTC) é o ato de se usar os mesmos bitcoins mais de uma vez em diferentes transações

primeiro bloco é chamado de “bloco gênese” e os demais blocos subsequentes possuem um *digest*[3] de seu bloco anterior, criando um histórico transparente e imutável de transações e registros nela armazenados [OLIVEIRA et al., 2019; FUJIMURA et al., 2015; ALECRIM, 2019].

Para garantir confiabilidade, quando um novo bloco é adicionado ao bloco anterior, é necessário um processo especial para solucionar um “quebra-cabeça”, chamado de Prova de Trabalho (*Proof-Of-Work*, POW). Esse processo ocorre para impedir que os invasores forjem essa Blockchain por conta própria. A maioria dos sistemas que utilizam a tecnologia Blockchain seguem o esquema POW como, por exemplo, a criptomoeda Bitcoin. Porém, existem outros esquemas de criação de blocos, como o *Proof-of-Stake* (PoS), o *Proof-of-Activity* (PoA) e o *Proof-of-Publication* (PoP) [OLIVEIRA et al., 2019; FUJIMURA et al., 2015].

A tecnologia Blockchain tem benefícios consideráveis em termos econômicos, políticos e legais; podendo ser aplicada nas mais diversas áreas como: finanças, saúde, imóveis, serviços públicos e setor governamental. Nesse sentido, esta tecnologia pode ser usada para trocar informações e realizar transações de ativos digitais em redes distribuídas. Além disso, serve de base para alteração de propriedades e armazenamento de informações e documentos importantes. Sendo assim, essa tecnologia é vista como uma das tendências tecnológicas mais importantes que influenciarão os negócios e a sociedade nos próximos anos, principalmente, devido a sua característica disruptiva e de grande potencial para as empresas e governos [ALECRIM, 2019; CHAGAS, 2019].

Dentre os principais benefícios desta tecnologia estão a promoção da transparência, segurança, confiança e controle; cujo foco é reduzir as fraudes e a corrupção, bem como proporcionar a rastreabilidade e auditabilidade com o objetivo de rastrear o histórico das transações e criar uma trilha de auditoria. Além disso, vale destacar as características de imutabilidade, inviolabilidade e resiliência desta tecnologia, pois uma vez que os dados forem registrados em Blockchain serão difíceis de serem excluídos ou alterados. Isso ocorre devido ao caráter de descentralização do sistema, que permite que apenas dados verificados por nós sejam aceitos através do mecanismo de consenso da rede, o que dificulta as tentativas de fraudes nas operações e nos dados [OLIVEIRA et al., 2019; FUJIMURA et al., 2015; ALECRIM, 2019; CHAGAS, 2019].

[3] Digest é o resultado de tamanho fixo da saída da função *hash*

Segundo [FUJIMURA et al. 2015] a tecnologia Blockchain tem um grande potencial de aplicação em sistemas de gerenciamento de direitos de vídeo, podendo controlar quais usuários têm direito de “reproduzir” ou “editar” esses vídeos, por exemplo. Atualmente, provedores de serviços de gerenciamento de direitos precisam gastar muito dinheiro para manter seus sistemas protegidos contra invasores e, consequentemente, os custos são inevitavelmente refletidos em suas taxas de serviços. Todavia, o sistema de gerenciamento de direitos baseado na tecnologia Blockchain possui uma estrutura forte contra ataques e seu provedor de serviços não tem a responsabilidade de manter a Blockchain sozinho, criando a possibilidade de reduzir as taxas de serviço aos usuários [FUJIMURA et al. 2015].

Além disso, é possível identificar que há diferenças entre o uso da tecnologia Blockchain para as criptomoedas e para o gerenciamento de direitos digitais; pois, nas criptomoedas, as informações trocadas entre os usuários são sobre trocas monetárias, já as informações nos sistemas de gerenciamento de direitos são sobre trocas de direitos ou licenças. Porém, ambos os tipos de informações devem ser registrados e transmitidos com segurança na Blockchain [FUJIMURA et al. 2015].

Um ponto importante a ser destacado é como tratar um arquivo de tamanho grande (capacidade alta de armazenamento) com segurança nos sistemas de gerenciamento de direitos digitais. De acordo com [FUJIMURA et al. 2015], se o tamanho médio dos arquivos for levado em consideração, tentar gravar os próprios arquivos na Blockchain é totalmente inapropriado. Portanto, os métodos para fornecer informações sobre os arquivos e direitos devem ser separados e combinados.

Na tecnologia Blockchain, segundo [FUJIMURA et al. 2015], é necessário um certo tempo (em média 10 minutos na criptomoeda Bitcoin) para adicionar uma nova transação como um novo bloco na Blockchain. E que, além disso, é altamente recomendável que a transação não seja aprovada até que seis blocos tenham sido acoplados após o bloco que inclui a transação de destino. Dessa forma, os usuários que usam a tecnologia Blockchain da mesma maneira que a criptomoeda Bitcoin são forçados a aguardar o uso do arquivo; mesmo que já tenha sido permitido pelo sistema de gerenciamento de direitos digitais. Logo, [FUJIMURA et al. 2015] destaca que é necessário criar uma maneira de reduzir esse atraso para refletir as informações de direitos na Blockchain.

Sendo assim, nota-se que a tecnologia Blockchain possui algumas limitações devido ao seu caráter distribuído, como por exemplo, a escalabilidade, a flexibilidade e

o tempo de resposta que são mais ineficientes se comparado às soluções tradicionais de banco de dados centralizados e, portanto, precisam ser melhoradas. Porém, percebe-se que seu potencial é notório e disruptivo, podendo ser usado em qualquer estrutura, permitindo reduzir custos e complexidade; além de compartilhar e garantir registros confiáveis. Todavia, as estruturas atuais deverão ser alteradas para permitir o gerenciamento de transações distribuídas com uma estrutura de controle para guiá-las [ALECRIM 2019].

2.4 – Contratos Inteligentes

Os Contratos Inteligentes surgiram como uma implementação promissora da tecnologia Blockchain. Porém, em 1994, o idealizador Nick Szabo [ALECRIM, 2019] já havia explorado a ideia de incorporar cláusulas contratuais a um protocolo computadorizado com o intuito de criar estruturas eficientes e autoexecutáveis, capazes de desestimular o descumprimento contratual e diminuir os custos de transação em relações formalizadas, com o auxílio de instrumentos digitais. Portanto, os Contratos Inteligentes são contratos digitais que permitem termos contingentes em consenso descentralizado, normalmente a prova de falsificação e auto reforçados por meio da execução automatizada. Desse modo, pode-se afirmar que a partir do surgimento da tecnologia Blockchain a abstração de Nick Szabo pode ser revivida e implementada de uma forma mais concreta, expressando não somente uma aplicação mais factível, como um atributo nuclear dos contratos digitais [OLIVEIRA, 2019; ALECRIM, 2019].

Atualmente, a aplicação prática dos direitos autorais tem se desdobrado em mecanismos autoritários de restrição do conhecimento através dos sistemas DRM, confrontando com as aspirações de liberdade e flexibilidade coerentes aos tempos interconectados em que se vive na sociedade [OLIVEIRA 2019]. Dessa forma, o surgimento dos Contratos Inteligentes se apresenta com grande potencial de aplicação em sistemas de DRM de modo a garantir os direitos dos ativos digitais sem prejudicar a liberdade do usuário [FUJIMURA et al. 2015].

Além disso, a programabilidade e a previsibilidade são características importantes da tecnologia Blockchain e que estão presentes nos Contratos

Inteligentes, podendo ser programados para serem autoexecutáveis [ALECRIM 2019].

No contexto da tecnologia Blockchain, os Contratos Inteligentes são trechos de códigos (scripts) armazenados na Blockchain que residem com um endereço único em uma cadeia de blocos; sendo capazes de operacionalizar registros complexos de propriedade de forma automatizada. No entanto, para que os Contratos Inteligentes sejam executados de maneira independente e automática em todos os nós da rede, os scripts deverão ser acionados quando se endereçar alguma transação para ele. Porém, só serão executados se as condições forem validadas por todos os nós da rede, tendo como premissa sua execução assegurada a partir do mecanismo imposto pelo protocolo de consenso. Sendo assim, pode-se dizer que cada nó na Blockchain que está habilitado por Contratos Inteligentes está executando uma máquina virtual e que a rede Blockchain atua como uma máquina virtual distribuída, conforme figura 5 [ALECRIM 2019].

O Contrato Inteligente define as regras e penalidades em torno de um contrato e executa e aplica automaticamente a obrigação no próprio contrato. Com isso, vale destacar que, como os termos de um Contrato Inteligente são interpretados por máquina, tendo em vista que seu núcleo é desenvolvido por código de software e seus termos são expressos em linguagens de computador, não há a possibilidade para duplas interpretações destes termos assim como ocorre com os contratos físicos (já que a mente humana utiliza critérios subjetivos). Desta forma, a precisão das linguagens de programação é capaz de evitar possíveis problemas associados à interpretação imprevisível de termos contratuais pela parte do contrato ou da agência de execução [ALECRIM 2019].

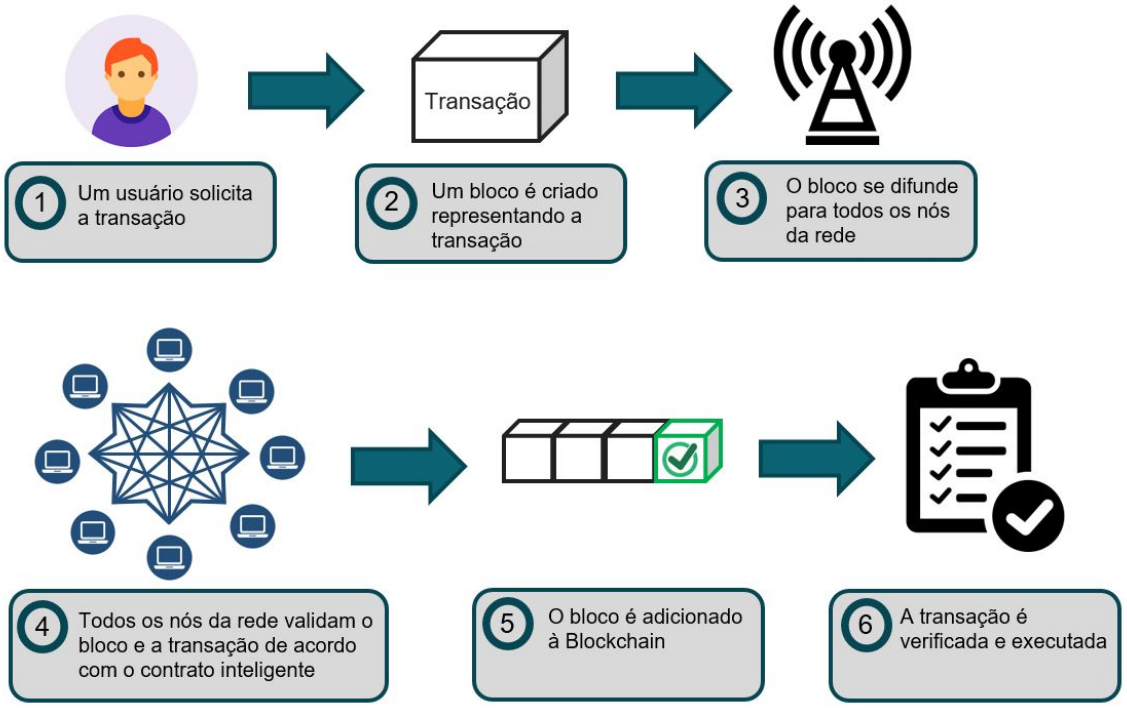


Figura 5. Funcionamento Blockchain e Contrato Inteligente

2.5 – Tecnologias utilizadas

Nesta seção são listadas algumas tecnologias de estudo que foram utilizadas na implementação do modelo proposto. São elas:

- **Node.js[4]:** é um ambiente de execução JavaScript server-side que trabalha em uma única thread de execução. Sendo assim, no modelo Node.js, apenas uma thread é responsável por tratar todas as requisições. Essa *thread* é chamada de *Event Loop*, e leva esse nome pelo fato de que cada requisição é tratada como um evento.
- **Ethereum[5]:** é uma plataforma de código aberto para desenvolvimento de aplicativos descentralizados; sendo a base para uma nova era na internet. Lançada em 2015, esta tecnologia é a principal blockchain programável do mundo. Todo programa que é executado na EVM (*Ethereum Virtual Machine*) é

[4] https://nodejs.org/en/
[5] https://ethereum.org/en/

chamado de *Smart Contract*, na qual, é desenvolvido popularmente através da linguagem de programação *Solidity*.

- **Ganache EVM[6] (Ethereum Virtual Machine):** é uma Blockchain pessoal para desenvolvimento rápido de aplicativos descentralizados da Ethereum, podendo ser utilizado em todo o ciclo de desenvolvimento; desde sua criação até a sua implementação e testes em um ambiente seguro e determinístico.
- **Solidity[7]:** é uma linguagem de programação de alto nível orientada a objetos para implementação de Contratos Inteligentes, sendo estaticamente tipada e com suporte a herança, bibliotecas e tipos complexos definidos pelo usuário.
- **Web3.js[8]:** é uma biblioteca que contém uma coleção de módulos com funcionalidades para o ecossistema Ethereum. Sendo assim, pode-se dizer que o Web3.js é uma API de Ethereum em JavaScript oferecendo uma interface conveniente para os métodos RPC (*Remote Procedure Call* - Chamada de Procedimento Remoto).
- **Truffle[9]:** é um *framework* utilizado para compilar os Contratos Inteligentes e, posteriormente, vincular e implantar esses Contratos Inteligentes no EVM; além de gerenciar os arquivos binários resultantes do processo de compilação.

[6] https://www.trufflesuite.com/ganache
[7] https://docs.soliditylang.org/en/v0.8.0/
[8] https://web3js.readthedocs.io/en/v1.3.0/
[9] https://www.trufflesuite.com/truffle

3 - Trabalhos Relacionados

Nesta seção serão apresentados os trabalhos relacionados que serviram como base ao modelo proposto de gerenciamento de direitos digitais através de Contratos Inteligentes.

3.1 – *Blockchain for digital rights management. Future Generation Computer Systems*

O trabalho [MA et al. 2018] apresenta um esquema baseado em Blockchain para gerenciamento de direitos digitais (DRM), cujo objetivo é fornecer proteção de conteúdo confiável de alto nível e rastreabilidade condicional do serviço de conteúdo de violação. Para isso foram utilizadas duas blockchains isoladas com interfaces ABI (*Contract Application Binary Interface*) para armazenar, respectivamente: informações resumidas simples e informações cifradas de conteúdo digital original protegido por DRM. Além de utilizar autenticação, proteção de privacidade e rastreabilidade condicional com base em várias assinaturas (no que diz respeito a licença DRM), controle de uso e informações de restrição que podem ser facilmente recuperadas do Blockchain; podendo ser consultado todo um histórico de consumo dos conteúdos digitais.

3.2 – *BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain*

O trabalho [FUJIMURA et al. 2015] apresenta um sistema de gerenciamento de direitos digitais baseado na tecnologia Blockchain, cujo objetivo é verificar e testar a aplicabilidade desta tecnologia na gestão dos direitos digitais. Foi construído em uma rede P2P onde existem três servidores de mineração, que é o menor número necessário para manter a cadeia de blocos. Nesse sistema, a mineração é o trabalho de cálculo realizado para conectar um novo bloco à Blockchain. Os nós do licenciante e do licenciado também participam da rede Blockchain, mas a mineração é realizada nesses nós. Esses nós são utilizados para emitir ou receber a transação e as informações sobre direitos, ou seja, licença de reprodução, estão incluídas na

transação emitida pelo licenciante.

O sistema de avaliação proposto por [FUJIMURA et al. 2015] leva em consideração a transferência da chave de licença necessária para decifrar vídeos criptografados. A criptografia do vídeo aumenta o nível de segurança e é garantido que o legítimo proprietário do vídeo emita a licença de uso, a não ser que a chave de licença tenha "vazado". Segundo [FUJIMURA et al. 2015], o ponto importante desse processo é usar a chave de criptografia pública e a chave secreta do licenciado para decifrar a chave de licença, fazendo com que somente ele tenha acesso. Sendo assim, de acordo com o sistema de avaliação, foi possível verificar o seguinte:

- O licenciante pode controlar a permissão de um determinado licenciado para usar um determinado vídeo;
- O licenciante pode alterar a permissão de um determinado licenciado para usar um vídeo específico em um determinado momento;
- Esses controles são ativados pelas informações de direitos na Blockchain e no software do player que segue essas informações.

3.3 – DLM: Uma proposta para empréstimo digital

Vale destacar que esse trabalho [OLIVEIRA et al. 2019] foi fruto da disciplina de Segurança e Auditoria de Sistemas no CEFET-RJ Campus Nova Friburgo, na qual, um dos autores foi o autor deste TCC. Sendo assim, a partir deste trabalho, foi gerado um artigo sobre Gestão de Direitos Digitais através de Contratos Inteligentes [OLIVEIRA e LAZARIN 2020] com o objetivo de manter o trabalho em crescente desenvolvimento através de novas tecnologias. Consequentemente, esses trabalhos foram um ensaio para a versão atual apresentada neste TCC.

O trabalho [OLIVEIRA et al. 2019] apresenta uma proposta para empréstimo e/ou venda de arquivos digitais entre os usuários, com o intuito de devolver a sensação de posse ao usuário sobre um determinado arquivo digital. A proposta visa dar mais liberdade de uso e transferência ao usuário e, simultaneamente, garantir os direitos da obra ao autor, evitando a prática da pirataria desses conteúdos na Internet. O trabalho apresenta um sistema inspirado em Blockchain onde cada transação de transferência de uma obra é registrada em um *livro razão*[10] no servidor para garantir a

[10] Base de dados onde serão registradas todas as transações de transferência ou empréstimo.

unicidade, rastreabilidade, confiabilidade e segurança do arquivo digital.

Este modelo está dividido em 3 membros: Controlador, Mediador e Usuário. O Controlador é responsável pelo controle de acesso, validação e garantia da identidade dos Usuários e Mediadores no sistema. Já o Mediador tem como objetivo incluir os arquivos digitais no sistema (sendo a entidade portadora do direito de cópia - copyright); validando, registrando e armazenando as informações sobre as atividades de transferência ou empréstimo desses arquivos segundo a confirmação de identidade do Usuário junto ao membro Controlador. E, por fim, o membro Usuário é uma entidade cadastrada no sistema que pode acessar ou transferir algum arquivo digital já cadastrado no sistema através do membro Mediador.

As garantias propostas por este modelo são:

- **Unicidade:** todo arquivo digital recebe um cabeçalho único e é criptografado por AES com uma chave aleatória gerada pelo sistema. Dessa forma, cada exemplar do arquivo digital se torna único e sua permissão de leitura, que necessita de acesso à chave criptográfica, é negociada entre Mediador e Usuário no sistema.
- **Rastreabilidade:** o Mediador através do seu processo de validação, registro e armazenamento de informações sobre as atividades de transferência ou empréstimos mantém o *livro razão* atualizado com a identificação atual (*hash*) e identificação anterior (*old hash*) de cada registro do arquivo digital no sistema. Sendo assim, é possível percorrer todo o encadeamento desses registros, construindo um histórico de todas as transações de cada arquivo digital.
- **Confiabilidade:** uma vez que o sistema proposto está inspirado no modelo de registro da tecnologia Blockchain, através do armazenamento de registros de transações no *livro razão* do próprio sistema, não será possível burlar o conteúdo de uma transação; pois, para isso, seria necessário alterar o digest de toda a cadeia de registros anteriores.
- **Segurança:** todo processo de transferência e/ou empréstimo passa por três etapas criptográficas:
    1. Utiliza-se o AES e uma chave gerada por um GNPA (Gerador de Número Pseudo-Aleatório);
    2. A chave aleatória é cifrada via RSA com a chave pública do Usuário fornecida pelo Controlador;

3. A chave resultante da etapa 2 acima e o arquivo digital são novamente cifrados via AES e uma chave conhecida pelo próprio sistema, garantindo assim a segurança na transmissão de arquivos entre os usuários.

3.4 – Comparativo

Sendo assim, pode-se dizer que o esquema apresentado em [MA et al. 2018] está mais focado na parte de segurança dos direitos digitais em detrimento da liberdade e flexibilidade no uso dos arquivos digitais pelo usuário. Já o sistema apresentado em [FUJIMURA et al. 2015] buscou implementar uma rede descentralizada Blockchain com o intuito de salvar a permissão do conteúdo digital nas transações realizadas na Blockchain sem a utilização de Contratos Inteligentes. Portanto, cada transação ficaria salva no livro razão de cada nó pertencente a rede. E, por fim, a proposta apresentada em [OLIVEIRA et al. 2019], apesar de ser um modelo que não utiliza Blockchain, sua estrutura é composta por um centralizador chamado Controlador (sem utilizar qualquer tipo de Contratos Inteligentes) com o objetivo de garantir ao usuário as permissões de acesso ao conteúdo digital.

Este trabalho, por sua vez, busca alinhar a ideia de empréstimo e/ou venda de arquivos digitais apresentadas por [OLIVEIRA et al. 2019] (com um membro Controlador) ao conceito de gerenciamento automático de direitos digitais apresentado por [MA et al. 2018], através dos Contratos Inteligentes. Sendo assim, cada permissão do conteúdo não seria salva em uma transação do livro razão, conforme [FUJIMURA et al. 2015], mas sim, seria salva no próprio contrato junto a Blockchain, para que tais transações sejam utilizadas posteriormente em validações junto ao membro Controlador do sistema.

4 - Proposta

Este trabalho apresenta um modelo de empréstimo digital baseado na tecnologia Blockchain, cujo objetivo é preservar os direitos autorais sem prejudicar a liberdade e flexibilidade do usuário do ativo digital, possibilitando a unicidade e a rastreabilidade de arquivos digitais, tornando o processo gerenciável, transparente e seguro.

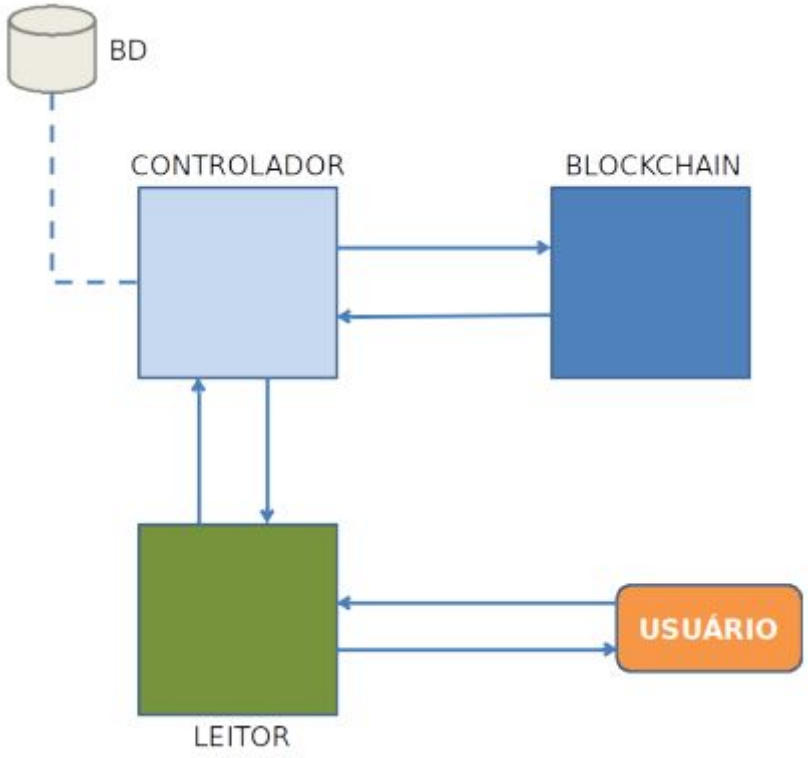


Figura 6. Modelo Proposto

A estrutura deste modelo é dividida em três membros: Controlador, responsável pelo processo de validação de empréstimo e/ou venda do arquivo digital; Leitor, responsável por atender as requisições de acesso do usuário aos arquivos digitais; e Blockchain, conforme apresentado na Figura 6. Abaixo são descritas as atribuições de cada membro.

- O **Controlador** é responsável por armazenar o arquivo original inserido pelo autor/editora e o arquivo cifrado (de forma a garantir a segurança de acesso ao conteúdo); gerar o par de chaves público/privada para o usuário acessar o

ativo digital posteriormente; gerar o *hash* do conteúdo do ativo digital (de forma a garantir a unicidade do arquivo); e registrar a transação na Blockchain.

- O **Leitor** é responsável por receber a requisição contendo as informações do *hash* do ativo digital e da carteira do usuário; validar as permissões do usuário, junto ao Controlador; e decifrar o arquivo digital recebido do Controlador através da chave privada do usuário.
- A **Blockchain** é responsável por armazenar os registros dos ativos digitais transacionados no modelo de empréstimo e garantir a segurança dessas transações.

Para utilizar o modelo proposto o usuário deverá realizar seu cadastro no Controlador e informar um endereço de carteira válido na Blockchain. Além disso, o cadastro de arquivo digital será feito pelo usuário diretamente no Controlador. Através do Leitor o usuário poderá transferir/emprestar um arquivo digital para outro usuário, informando o *hash* da transação que garante sua propriedade sobre o ativo digital e a identificação das carteiras de origem e destino; bem como informar a data de validade de empréstimo caso a transferência não seja uma venda ou revenda. Dessa forma, o Leitor enviará a requisição ao Controlador que irá validar e posteriormente registrar a transação junto a Blockchain, armazenando os campos conforme Figura 7.

Campo	Descrição
hashObra	Identificação única da obra
Owner	Dono do arquivo
Deadline	Validade de empréstimo
Datetime	Data/hora de realização da transação
User	Usuário que possui o direito de acesso

Figura 7. Campos registrados na Blockchain

Vale destacar que o Contrato Inteligente é imprescindível para que os registros de licença dos arquivos digitais sejam salvos na Blockchain. Sendo assim, antes de qualquer transação no modelo, necessitamos fazer o upload do contrato para a Blockchain em uma transação do tipo “*contract*”, registrando que toda a transação de arquivo digital que ocorrer após o bloco “*contract*” utilize toda a verificação descrita neste contrato digital.

O modelo proposto visa garantir: Unicidade, Rastreabilidade e Segurança na troca de arquivos digitais, através das etapas descritas abaixo:

- **Unicidade:** todo arquivo inserido no Controlador terá um *hash* único da transação com as informações do arquivo e será cifrado utilizando um algoritmo simétrico de bloco com uma chave aleatória, tornando cada exemplar transacionado único no sistema.
- **Rastreabilidade:** uma vez que o modelo é baseado em Blockchain não é possível negar a transação realizada. Através do *hash* transação será possível identificar os metadados do arquivo, tais como: dono, usuário com permissão de acesso, data de cadastro do arquivo e prazo de empréstimo, etc.
- **Segurança:** todo acesso aos arquivos digitais e a comunicação entre os servidores envolvidos passa por diversas etapas criptográficas.

O processo criptográfico para garantia da segurança é dividido entre os membros Controlador e Leitor. O Controlador cifra o arquivo original gerando um exemplar e uma chave de acesso. O Leitor requisita o exemplar e a chave de acesso ao Controlador e com a chave privada do usuário decifra o exemplar para visualização. Na Figura 8 são apresentados os processos realizados no Controlador e no Leitor. Abaixo são descritas as etapas do processo:

- **Pré-requisitos:**

1. O Controlador e o Leitor devem possuir uma chave privada, secreta e única para o sistema (*SystemKey*);
2. O Usuário deve possuir um par de chaves (público/privado);

- **Processo de cifragem realizado no Controlador**

1. A cada transação é gerada uma chave privada aleatória;
2. O arquivo digital é cifrado utilizando um algoritmo simétrico de bloco com a chave aleatória gerada;
3. A saída da etapa anterior é novamente criptografada com a chave única do sistema, resultando no exemplar único do arquivo original.
4. A chave aleatória é cifrada utilizando um algoritmo criptográfico assimétrico com a chave pública do usuário;

5. A saída da etapa anterior é novamente criptografada com a chave única do sistema, resultando na chave de acesso ao exemplar;
6. O exemplar e a chave de acesso são armazenados no Controlador com o nome da identificação da carteira do usuário e o *hash* da transação. Além disso, o Controlador registra todos os dados (vide Figura 7) na Blockchain para futuras validações.

- **Processo de decifragem realizado no Leitor**

1. Requisição ao Controlador do exemplar e da chave de acesso, verificando a permissão de acesso do usuário junto a Blockchain;
2. A chave de acesso é decifrada utilizando chave privada única do sistema;
3. A saída da etapa anterior é decifrada por um algoritmo criptográfico assimétrico, utilizando a chave privada do usuário.
4. O exemplar é decifrado utilizando chave privada única do sistema;
5. A saída da etapa anterior é novamente decifrada utilizando a saída do algoritmo assimétrico, resultando no conteúdo original.

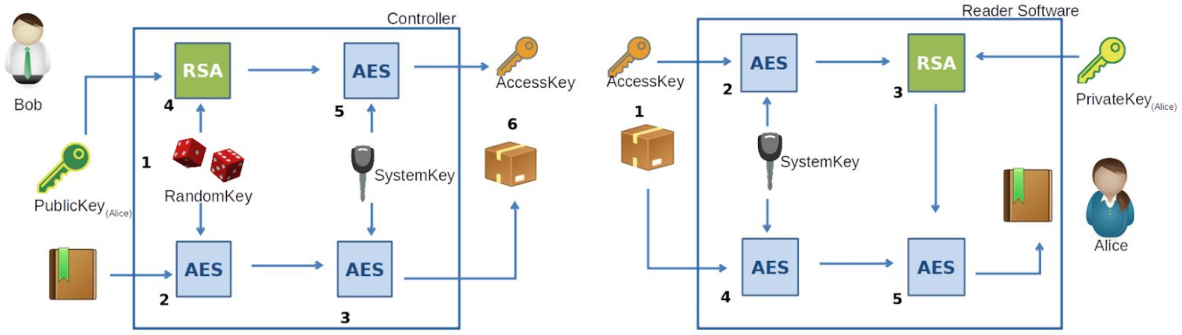


Figura 8. Processo criptográfico para proteção do conteúdo

4.1 – Implementação

Como prova de conceito, o modelo proposto foi implementado em Node.js, um ambiente de execução Javascript *server-side*. A linguagem de programação adotada para implementar os membros Controlador e Leitor foi o JavaScript. Já para o membro

Blockchain foi utilizado o Ganache EVM[11] (*Ethereum Virtual Machine*), uma blockchain pessoal da Ethereum que pode ser utilizada para executar testes, comandos e inspecionar as operações da cadeia de blocos. Na implementação apresentada na Figura 9 foi possível realizar as transações referentes às permissões do empréstimo e/ou revenda dos arquivos digitais, simulando a dinâmica de funcionamento do modelo.

Além disso, foi utilizado o *framework* Truffle[12] para compilar e fazer o upload do Contrato Inteligente para o Ganache EVM. O Contrato Inteligente foi descrito em Solidity[13], uma linguagem de programação de alto nível, orientada a contratos. Por fim, para que o membro Controlador pudesse se comunicar à Blockchain, foi necessário utilizar a API Ethereum JavaScript Web3.js[14], que permite integração com um nó Ethereum local ou remoto, usando conexões HTTP ou IPC.

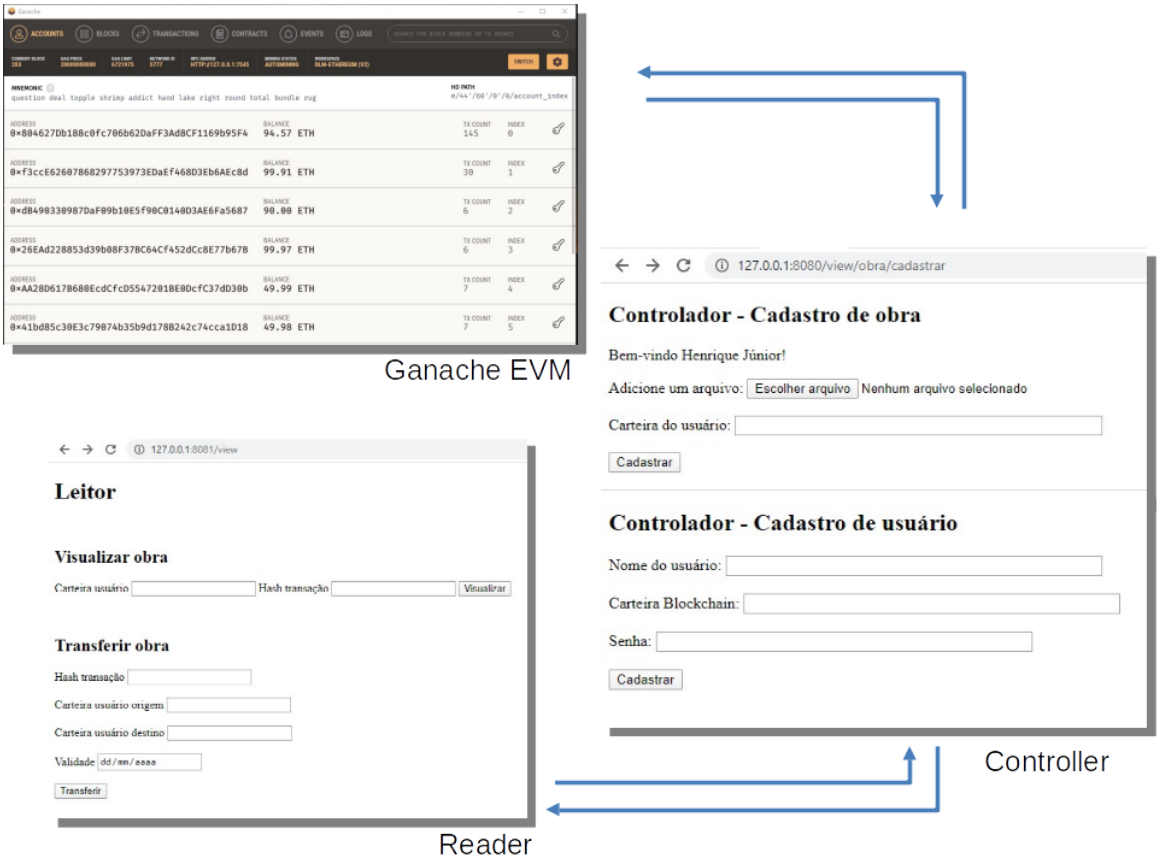


Figura 9. Implementação

[11] https://www.trufflesuite.com/ganache
[12] https://www.trufflesuite.com/truffle
[13] https://docs.soliditylang.org/en/v0.8.0/
[14] https://web3js.readthedocs.io/en/v1.3.0/

4.1.1 – Cadastro do usuário no sistema

O cadastro do usuário ocorre no membro Controlador do sistema e deverão ser informados os seguintes dados: nome de usuário, uma identificação válida da carteira Blockchain e senha do usuário.

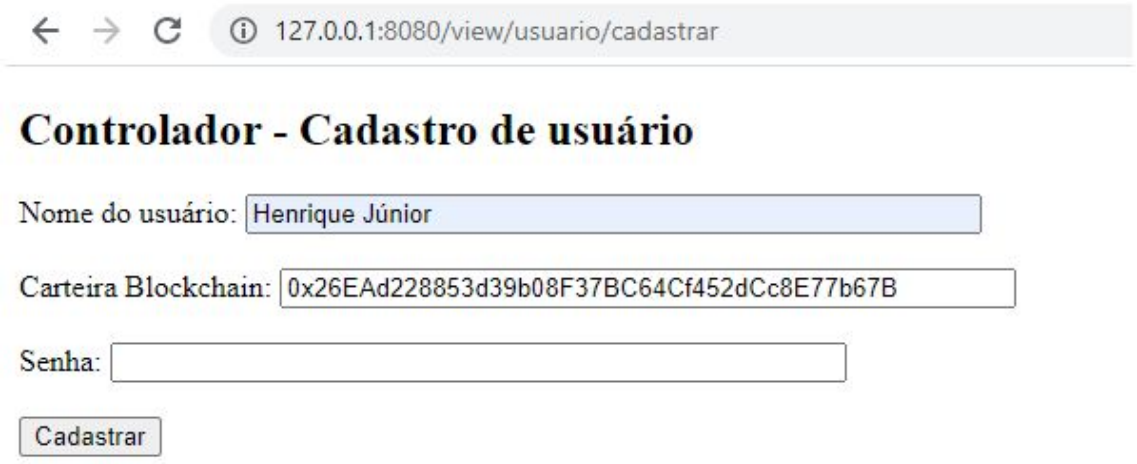


Figura 10. Tela de cadastro do usuário

Sendo assim, o sistema irá gerar um repositório com a identificação da carteira do usuário no membro Controlador.

4.1.2 – Cadastro do ativo digital no sistema

Para o cadastro do ativo digital no membro Controlador do sistema é necessário fazer o upload do arquivo e adicionar a identificação da carteira do usuário (Figura 11) que, de imediato, será o dono e o usuário com permissão de acesso ao conteúdo.

Sendo assim, o sistema irá gerar um *hash* do conteúdo do ativo digital para a identificação de um novo repositório, que será criado dentro do repositório que identifica a carteira do usuário. Logo, cada ativo digital poderá ser encontrado mais facilmente dentro de cada carteira do usuário.

Figura 11. Tela de cadastro do ativo digital

Além disso, o sistema irá gerar um par de chaves público e privada para o usuário, para que o conteúdo do arquivo possa ser cifrado no membro Controlador e decifrado no membro Leitor.

Vale destacar ainda que o conteúdo do arquivo cifrado com a chave pública do usuário será salvo dentro do repositório identificado com o *hash* do conteúdo do arquivo original e o membro Controlador enviará os dados para registro (vide Figura 7) ao membro Blockchain. A Blockchain, por sua vez, registrará os dados e retornará o *hash* da transação do ativo digital para posteriores acessos do usuário.

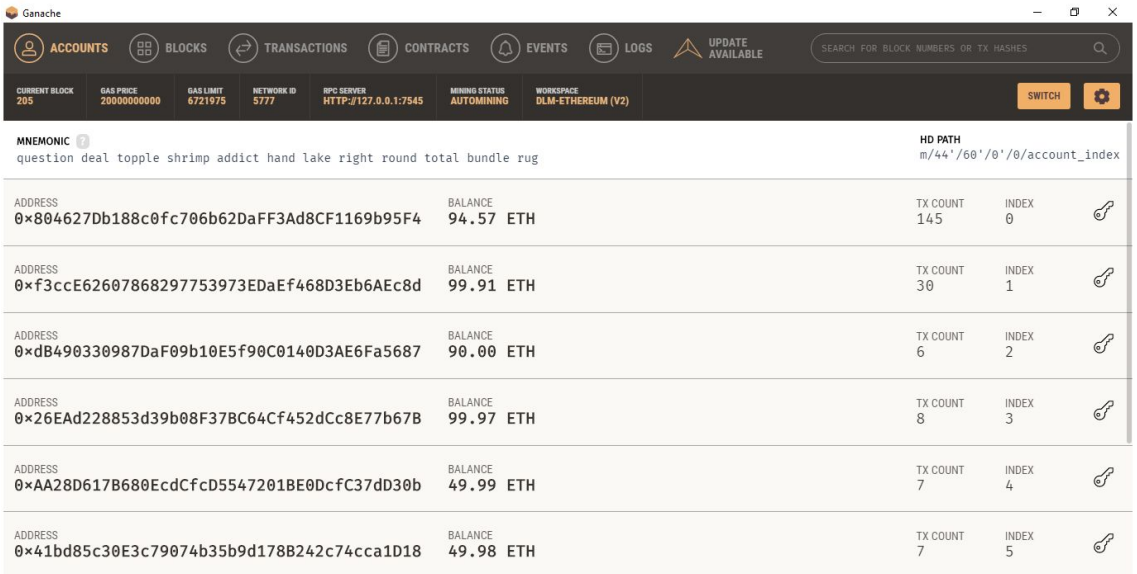


Figura 12. Tela de carteiras da Blockchain com o Ganache EVM

Sendo assim, somente a chave privada deste usuário com permissão de acesso será capaz de decifrar o conteúdo do arquivo no membro Leitor.

4.1.3 – Transferência de arquivos entre os usuários do sistema

O processo para empréstimo e/ou venda e revenda é o mesmo. A diferença é que no processo de empréstimo deverá ser informada a data de validade do empréstimo (*Deadline*), vide Figura 7. Já com o processo de venda ou revenda o campo *Deadline* deverá ficar nulo.

Para realizar a transferência de arquivos, o usuário deverá inserir os seguintes dados no membro Leitor: *hash* da transação do arquivo na Blockchain, identificação da carteira do usuário de origem, identificação da carteira do usuário de destino e data de validade do empréstimo (caso seja uma transferência de empréstimo).

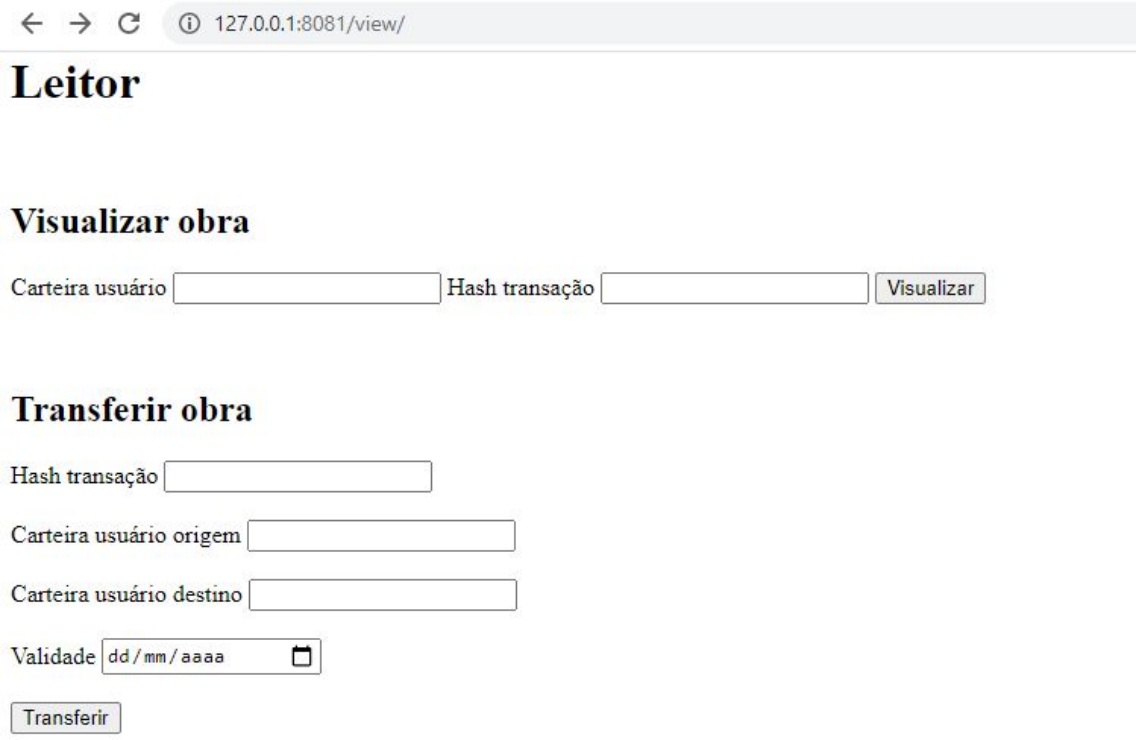


Figura 13. Tela do Leitor para visualização e/ou transferência do ativo digital

Portanto, após realizada a transferência, a Blockchain retornará um novo *hash* de transação para o arquivo, na qual, constará as novas permissões de acesso como: *user* (usuário com permissão de acesso), *owner* (dono do arquivo) e *deadline* (validade de empréstimo).

4.1.4 – Visualização de arquivos pelos usuários do sistema

Para o usuário poder visualizar o conteúdo do arquivo de forma legível no membro Leitor, ou seja, com o conteúdo decifrado, o usuário deverá inserir a identificação da carteira do usuário na Blockchain e o *hash* da transação do arquivo na Blockchain (vide Figura 13). No entanto, o membro Controlador fará as validações de permissão do usuário junto ao Contrato Inteligente na Blockchain para verificar se o arquivo poderá ser visualizado pelo usuário que está tentando acessá-lo.

Caso o usuário tenha permissão de acesso, o membro Leitor irá decifrar o conteúdo do arquivo e retornará o conteúdo legível ao usuário (vide Figura 8).

4.2 – Comparativo: Modelo proposto x DRMs existentes

Atualmente existem algumas empresas no mercado, como a Amazon com o Kindle, a Apple com o iBooks e a Google com o Play Livros que investem em tecnologias de *Digital Rights Management* (DRM) próprios para disponibilizarem o conteúdo apenas para quem possui permissão para consumí-lo; com o intuito de evitar acessos ou cópias ilegais deste conteúdo digital. Porém, a utilização dessa tecnologia tem sido muito debatida nas comunidades espalhadas pela internet, pois, a partir do momento em que o conteúdo adquirido pelo usuário possui limitações, este começa a questionar se ele realmente tem posse desse conteúdo (como seria em um produto físico, por exemplo), de tal forma que aquele que o adquiriu pode emprestar, doar ou revender [OLIVEIRA et al. 2019].

Sendo assim, há várias incertezas que abarcam os usuários, principalmente nos aspectos relacionados com os negócios digitais; como por exemplo: O que é permitido acessar? O que se pode fazer em relação aos conteúdos? Quantos podem ler ao mesmo tempo? Quais as vantagens oriundas da aquisição de livros digitais? Quais as dificuldades na relação biblioteca-editor-cliente em relação aos e-books? Como emprestar esse suporte informacional? [OLIVEIRA et al. 2019].

Na Tabela 1 é apresentado um comparativo entre o modelo proposto e os DRMs utilizados pelas plataformas Play Livros, Kindle e iBooks.

Tabela 1- Comparativo entre alguns DRMs e o modelo proposto

Garantias	Modelo Proposto	Play Livros	Kindle	iBooks
Direitos autorais (digitais)	Sim	Sim	Sim	Sim
Compra do conteúdo digital	Sim	Sim	Sim	Sim
Venda do conteúdo digital	Sim	Não	Não	Não
Empréstimo entre usuários	Sim	Não	Sim	Não
Rastreabilidade	Sim	Não	Não	Não

Pode-se destacar algumas vantagens do modelo proposto, sendo elas [OLIVEIRA et al. 2019]:

1) Os direitos autorais e o processo de transferência de compra são garantidos por todos. Porém, apenas no Modelo Proposto um usuário poderá comprar um livro de outro usuário (proprietário);
2) A transferência de propriedade cria uma economia de arquivos digitais, possibilitando a existência de sebos digitais;
3) O empréstimo entre usuários soluciona o problema da expansão no uso dos e-books por bibliotecas públicas, por exemplo;
4) Implementa a tecnologia Blockchain em suas transações, garantindo a rastreabilidade e transparência no processo de empréstimo digital;
5) Devolve ao leitor a sensação de posse, uma vez que o mesmo pode emprestar, doar ou revender.

No entanto, há algumas desvantagens do Modelo Proposto, como por exemplo:

1) O tempo de validação do processo de empréstimo e/ou venda pode ser demorado. Pois, de acordo com [FUJIMURA et al. 2015], com a tecnologia Blockchain é necessário um certo tempo para adicionar uma nova transação como um novo bloco na Blockchain. E que, além disso, é altamente recomendável que a transação não seja aprovada até que seis blocos tenham sido acoplados após o bloco que inclui a transação de destino;
2) O Modelo Proposto possui um membro Controlador trabalhando com uma tecnologia distribuída e descentralizada; podendo ter um impacto negativo a

nível de escalabilidade do sistema;

3) Atualmente, o Modelo Proposto possui uma chave única do sistema (*SystemKey*) para garantir que tanto o processo de cifrar quanto de decifrar estejam sendo feitos pelo próprio Modelo Proposto. Ou seja, os ativos digitais só poderão ser visualizados pelo sistema proposto através do membro Leitor, o que pode ser uma desvantagem para os usuários.

5 - Considerações Finais

Atualmente, a aplicação prática dos sistemas de DRM tem se efetivado em mecanismos de controle e restrição, limitando a sensação de posse do usuário de um determinado arquivo digital [OLIVEIRA et al., 2019; OLIVEIRA, 2019].

Entretanto, o surgimento dos Contratos Inteligentes se apresenta com grande potencial de aplicação em sistemas de DRM de modo a garantir os direitos dos ativos digitais sem prejudicar a liberdade do usuário [FUJIMURA et al. 2015]. A Blockchain e os Contratos Inteligentes são novas ferramentas tecnológicas que deverão ser direcionadas para reforçar a posição pela liberdade de informação, e, consequentemente, pela visão do direito de autor como um meio de difusão de cultura e conhecimento [LANA 2019].

O objetivo deste trabalho foi apresentar um modelo de gestão de direitos de ativos digitais através das tecnologias Blockchain e Contratos Inteligentes com o intuito de controlar o nível de permissão de acesso, leitura e transferência do conteúdo dado ao usuário final e garantir a unicidade do ativo digital; possibilitando o empréstimo e/ou revenda desses ativos digitais pela internet. Logo, utilizou-se dessas tecnologias emergentes no mercado e que são promissoras nesse desafio que é garantir os direitos autorais do ativo digital sem ferir a liberdade de uso do usuário que o adquiriu. Portanto, o modelo proposto neste trabalho busca alinhar a ideia de empréstimo e/ou venda de arquivos digitais apresentadas por [OLIVEIRA et al. 2019] ao conceito de gerenciamento automático de direitos digitais apresentado por [MA et al. 2018], evoluindo a proposta de [FUJIMURA et al. 2015] através dos Contratos Inteligentes.

Desse modo, acredita-se que o modelo proposto poderá contribuir com os autores/editoras e o mercado de e-books, uma vez que, os investimentos realizados para garantir a segurança de tais ativos digitais diminuiria, devido ao menor esforço estabelecido pela tecnologia Blockchain, além de possibilitar a autores/editoras identificar, através da rastreabilidade, como determinado ativo digital tem sido transacionado na Internet, permitindo tirar conclusões para tomada de decisões a nível de negócio.

5.1 – Trabalhos futuros

Este trabalho abre um leque de opções de trabalhos futuros tanto nas áreas da Tecnologia da Informação quanto na área de Direito.

Na área de Tecnologia da Informação ainda poderão ser analisados e estudados como o modelo DLM proposto irá se comportar em um ambiente real de transações junto a Blockchain; levando-se em conta os custos transacionais em valores monetários entre cada usuário e os custos computacionais em relação a hardware, no que diz respeito a capacidade de armazenamento, velocidade de transferência e carga de recebimento de requisições. Além disso, será necessário avaliar o custo x benefício do modelo DLM sobre o nível de segurança do sistema adotado e avaliar a escalabilidade sobre o potencial crescimento do modelo.

Como o modelo proposto está atrelado a uma chave única do sistema, chamada de *SystemKey,* os ativos digitais só podem ser visualizados pelo próprio sistema proposto. Sendo assim, será necessário analisar o nível de aceitação entre a comunidade e verificar se há uma outra forma de, por exemplo, os softwares DRM existentes no mercado aderirem o modelo DLM com suas próprias chaves privadas; garantindo que cada software DRM tenha seu próprio nível de segurança no sistema DLM.

Na área de Direito é preciso ser estudado a Lei Geral de Proteção de Dados Pessoais (LGPD) n° 13.709/18 e a relação entre os Direitos Autorais e os Direitos do Consumidor para que o processo de transferência dos ativos digitais estejam dentro da lei nacional e/ou internacional.

Referências

National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES). Federal Information Processing Standards Publication (NIST FIPS - 197), 2001. Disponível em: <https://csrc.nist.gov/publications/detail/fips/197/final>. Acesso em 23 de dez. de 2020.

ALECRIM, J. d. S. C. (2019). Análise Crítica da Sistemática de compras Governamental pela Perspectiva de Novas Tecnologias de Contratos Inteligentes. Dissertação (Mestrado em Gestão do Conhecimento e Tecnologia da Informação) - Universidade Católica de Brasília, page 136 f.

BECKER, Eberhard & BUHSE, Willms & GUNNEWIG, Dirk & RUMP, Niels. Digital Rights Management: Technological, Economic, Legal and Political Aspects, 2003, Springer.

CHAGAS, Edgar Thiago de Oliveira. Blockchain: a revolução tecnológica e impactos para a economia. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 04, Ed. 03, Vol. 07, pp. 110-144. Março de 2019. ISSN: 2448-0959.

FUJIMURA, S., WATANABE, H., NAKADAIRA, A., YAMADA, T., and AKUTSU, A. (2015). BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain. 2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin).

GALLO, Michael A., HANCOCK, Willian M. Comunicação entre computadores e tecnologias de rede / Michael A. Gallo, Willian M. Hancock - São Paulo: Pioneira Thomson Learning, 2003.

IANZEN, A., PINTO, J. S. P., and WILDAUER, E. W. (2013). Os sistemas de proteção de direito digital (DRM): tecnologias e tendências para e-books. Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, v. 18(n. 36):p. 203–230.

KIM, David. Fundamentos de segurança de sistemas de informação / David Kim, Michael G. Solomon. - 1. ed. - Rio de Janeiro : LTC, 2014.

LANA, PEDRO. A possibilidade de contratos inteligentes no licenciamento de direitos de autor em Portugal (The Possibility of Smart Contracts In Copyright Licensing in

Portugal) (January 11, 2019). Anais do XIII Congresso de Direito de Autor e Interesse Público, Curitiba: GEDAI, 2020, Available at SSRN: https://ssrn.com/abstract=3618738

LAZARIN, Nilson Mori. Método não supervisionado de reconhecimento de padrões criptográficos/ Nilson Mori Lazarin; orientado por José Antônio Moreira Xexéo. Rio de Janeiro: Instituto Militar de Engenharia, 2012.

MA, Z., Jiang, M., Gao, H., and Wang, Z. (2018). Blockchain for digital rights management. Future Generation Computer Systems, 89:746 – 764.

MORAES, Thiago Gonçalves (2014). O Impacto das Tecnologias DRM no Direito do Consumidor. Monografia (Bacharelado em Ciência da Computação). Universidade Federal do Maranhão. 64.p

OLIVEIRA, Henrique Júnior de Souza; LAZARIN, Nilson Mori. Gestão de Direitos Digitais através de Contratos Inteligentes. In: WORKSHOP DE TRABALHOS DE INICIAÇÃO CIENTÍFICA E DE GRADUAÇÃO - SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 38. , 2020, Rio de Janeiro. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020 . p. 225-232. ISSN 2177-9384.

OLIVEIRA, H. J. S., PEREIRA, R. C., MACHADO, W. P., and LAZARIN, N. M. (2019). DLM: Uma Proposta para Empréstimo Digital. Computer on The Beach 2019, pages p. 238–247.

OLIVEIRA, J. V. (2019). O FUTURO REPETINDO O PASSADO? DIGITAL RIGHTS MANAGEMENT, tecnologias DISRUPTIVAS E O DIREITO AUTORAL BRASILEIRO. Quaestio Iuris, v.12:pp. 647–672.

RFC 1321. The MD5 Message-Digest Algorithm, 1992. Disponível em: <https://www.rfc-editor.org/info/rfc1321>. Acesso em: 23 de dez. de 2020.

SECURE HASH STANDARD. Federal Information Processing Standards Publication 180-1 (FIPS 180-1), 1995. Disponível em: <http://www.umich.edu/~x509/ssleay/fip180/fip180-1.htm>. Acesso em: 23 de dez. de 2020.

TANENBAUM, Andrew S., 1944 - Redes de computadores / Andrew S. Tanenbaum. - Rio de Janeiro : Elsevier, 2003.

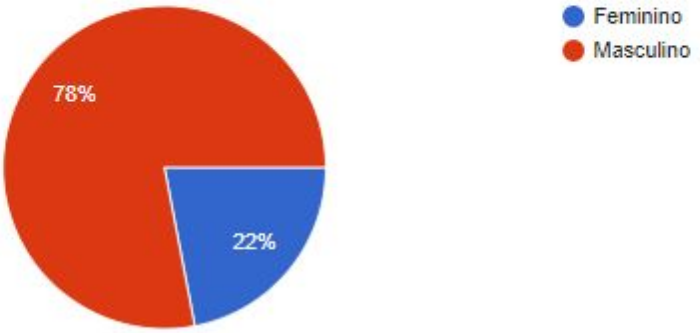
TERADA, Routo. Segurança de Dados: criptografia em redes de computador - São

Paulo: Blucher, 2008.

APÊNDICE A - Pesquisa de campo sobre a aceitação de público do modelo proposto

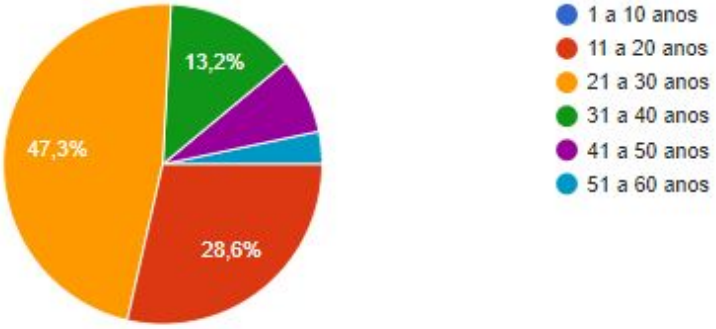
Qual é o seu sexo?

91 respostas



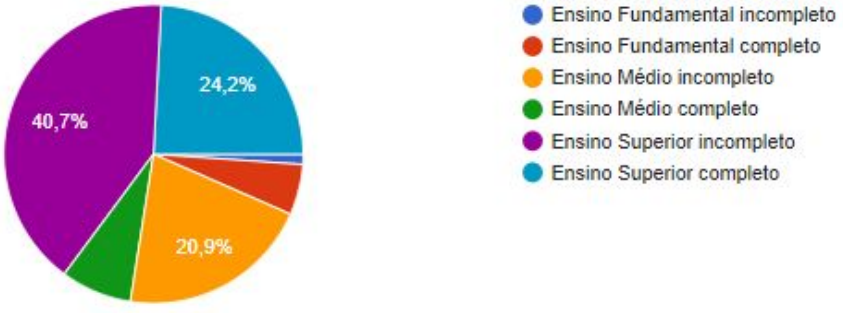
Sua idade está entre:

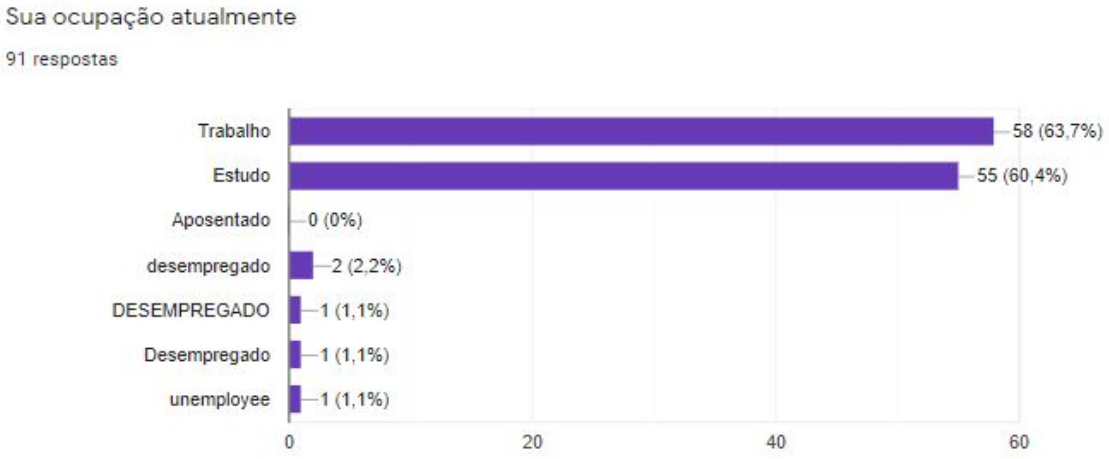
91 respostas

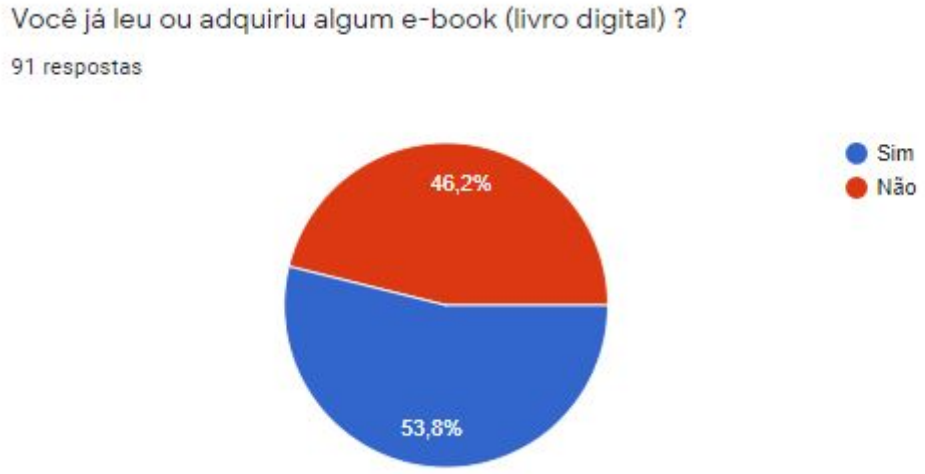


Sua formação escolar:

91 respostas







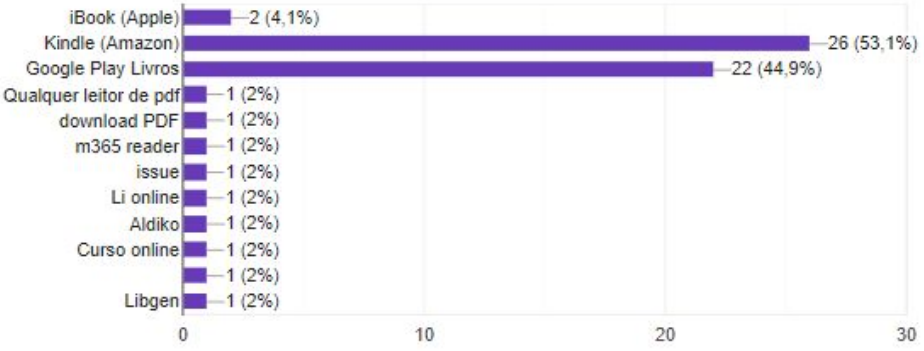
Com esta última pergunta acima, conseguiríamos identificar quem já teve contato com um livro digital e quem ainda não teve contato. Sendo assim, dividimos a seção em 2 partes:

1. Perguntas sobre o E-book para aqueles que já leram um livro digital;
2. Pergunta sobre o motivo das outras pessoas ainda não terem contato com livro digital.

- **Perguntas sobre o E-book**

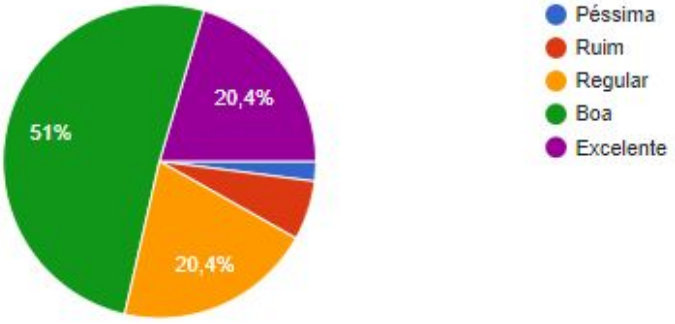
Qual plataforma digital você utilizou para ler o e-book?

49 respostas



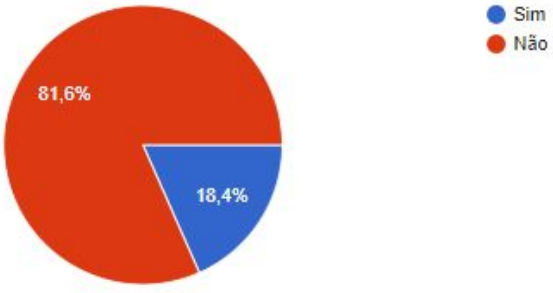
Sua experiência com e-book foi:

49 respostas



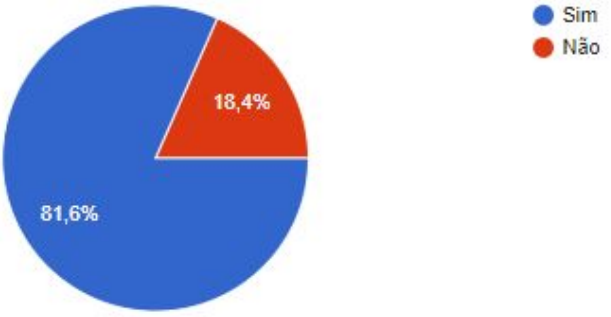
A plataforma do e-book permitia que você pudesse emprestar o e-book para um amigo seu, por exemplo?

49 respostas



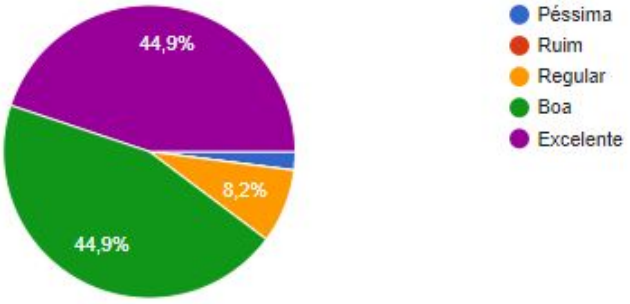
Você gostaria de emprestar ou de pegar emprestado um e-book com alguém?

49 respostas



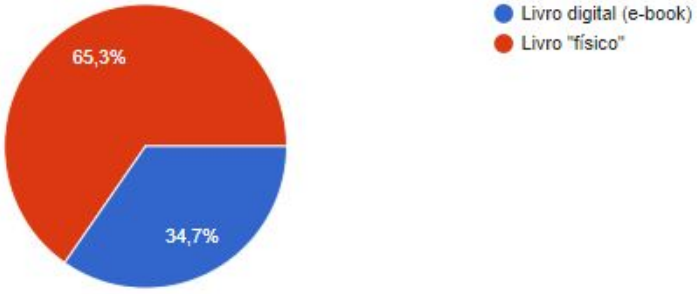
Sobre empréstimo de e-book (entre amigos, por exemplo), você acha que a ideia é:

49 respostas



Você prefere ler um livro digital (e-book) ou um livro "físico"?

49 respostas



Descreva o motivo pela qual você prefere um "livro digital" ou um "livro físico":	Motivo pela qual você ainda não leu ou adquiriu um e-book:
Gosto da sensação de folhear livros e gosto de colecionar.	Nunca tive interesse por e-books
Praticidade de poder ler em qualquer lugar e em dispositivos diferentes	Prefiro livro físico
Consigo me localizar melhor nas marcações que faço, é palpável.	Não gosto de ler
Digital, Praticidade de transporte	Prefiro livro físico
Mais confortável, nostálgico	Nunca tive interesse por e-books, Prefiro livro físico, Não gosto de ler
Facilidade de acesso rápido.	Prefiro livro físico
Praticidade, custo	Não gosto de ler
Segurança, melhor leitura	Prefiro livro físico
Gosto da sensação de ter o livro nas mãos	Não gosto de ler
Não ocupa espaço e pelo meio ambiente.	Nunca tive interesse por e-books
O livro físico é mais confortável para ler	Prefiro livro físico
Usabilidade	Prefiro livro físico

Segurança, melhor leitura	Não gosto de ler
Poder rabiscar	Prefiro livro físico
Lendo muito tempo um livro digital me dá dor nas vistas, por isso prefiro físico.	Prefiro livro físico
Praticidade e mobilidade	Não gosto de ler
folhear as páginas	Não gosto de ler
Não cansa a vista	Não gosto de ler
Me atrai a atenção o livro físico principalmente pela textura das folhas	Prefiro livro físico
Porque o livro digital não é necessário carregar peso	Não gosto de ler
Na verdade, depende do livro. Livros técnicos prefiro e-book. Outros temas prefiro físico	Prefiro livro físico
Prefiro o livro digital pela facilidade de transporte, posso ter vários no celular. Além disso, os apps possuem várias funcionalidades úteis, como a de dicionário e flashcards.	Prefiro livro físico
Manusear e fazer a anotações	Prefiro livro físico
O contato com livros físicos é estimulante e, simplesmente por não representar danos à visão, se sobrepõe aos digitais.	Nunca tive interesse por e-books
O livro físico é menos danoso aos olhos e transmite mais emoções.	Prefiro livro físico

Porque ele fica com você, e pelo celular você pode se distrair com outras coisas!	Prefiro livro físico
Tamanho da letra, mobilidade e conforto de manuseio do livro.(desktop é fixo, celular móvel, mas letra é pequena, e notebook é móvel e tem a letra grande, mas é mais difícil de manusear do que um livro e te dá menos possibilidade de posições de leitura)	Prefiro livro físico
Praticidade	Prefiro livro físico, Não gosto de ler
prefiro livro digital pela praticidade	Prefiro livro físico
As páginas de um livro físico não prejudicam minha visão como as de um livro digital acessado por um aparelho eletrônico.	Nunca tive interesse por e-books, Prefiro livro físico
Meus olhos se cansam mais rápido quando estou lendo algo no computador ou no celular.	Prefiro livro físico
Minha concentração na leitura é acentuada em livros físicos.	Prefiro livro físico, As permissões de acesso ao e-book são muito restritas
Praticidade	Nunca tive interesse por e-books
Praticidade	Nunca tive interesse por e-books, Prefiro livro físico

Por espaço e variedade	Nunca tive interesse por e-books
Prefiro o livro físico, pois ao ler um livro digital existem vários fatores que podem desviar a atenção. Além de que o livro físico é muito mais confortável para a visão do que o e-book.	Não sabia o que era "e-book"
Carrego todos meus livros em um único aparelho leve. Não ocupa espaço na minha casa (nem tenho esse espaço para ocupar, na verdade). No Kindle tenho todas as funcionalidades do livro físico, como fazer grifos, anotações e marcar páginas. Além disso, tenho funcionalidades extras como dicionário embutido (ótimo para ler livros em outros idiomas), busca por texto e iluminação do dispositivo. E-books também costumam ser bem mais baratos que o livro físico. Ao comprar o livro digital já tenho acesso imediato a ele. Se fosse comprar um livro físico pela internet, precisaria esperar chegar e pagar frete em alguns casos.	Prefiro livro físico, As permissões de acesso ao e-book são muito restritas, Pretendo ler e-books à partir de um Kindle e no momento não posso adquirir um
Costume de ter o livro em mãos, fora o modo de leitura, embora o e-Reader simule páginas, não é a mesma coisa	Prefiro livro físico
Praticidade	Prefiro livro físico
Computador gera distrações.	Nunca tive interesse por e-books, Prefiro livro físico, Não gosto de ler
Tenho costume de ler livros físicos.	Prefiro livro físico

Primeiro acho que a plataforma de e-books ainda precisa melhorar muito. Tenho uma relação com livro físico (p.ex. fazer marcações , escrever comentários na lateral do livro, poder alternar entre duas ou mais páginas etc.) que ainda não existe nas plataformas visuais. Segundo, acho que o preço dos livros virtuais ainda é comparativamente muito caro em relação ao impresso, uma vez que os livros físicos possuem um custo muito maior (transporte, impressão, ...) que os livros virtuais.	Não sabia o que era "e-book"
Instintivo, não te deixa dependente de uma máquina para acessar!	
Materialização da abstração, sentimento de posse, cheiro.	
Livros digitais permitem que você carregue uma biblioteca consigo. O livro digital também facilita o acesso à leitura. Por exemplo, fica mais fácil de ler nos momentos ociosos do dia-a-dia, como em filas de banco, pontos de ônibus, etc.	
Apego	
Não tenho um Kindle e, por isso, dói a vista ler em outros dispositivos	
Não sou nativo digital	
Posso carregar minha coleção no telefone/tablet/e-reader. Possibilidade de ler à noite com as luzes apagadas	

- **Pergunta sobre o motivo das outras pessoas ainda não terem contato com livro digital**

E, a última pergunta abaixo foi feita para todas as pessoas: