DLM: Uma proposta para empréstimo digital

Henrique J. S. Oliveira, Renato C. Pereira, Wender P. Machado
Nilson Mori Lazarin

[1]Bacharelado em Sistemas de Informação
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ)
Nova Friburgo, RJ – Brasil

{henriquejuniorfla,renatopereira.wp,wenderpmachado}@gmail.com

nilson.lazarin@cefet-rj.br

Abstract. *This paper shows a Digital Rights Management (DRM) model inspired on blockchain that protect the copyright and guarantee the singularity, log, trust and security of digital files. This model allows users to resell or lend digital files without infringing on copyright and presents itself as a solution for libraries to manage the loan of digital files. Finally, an application was developed to prove the concept of the model also a comparative with other DRM is presented.*

Resumo. *Este trabalho apresenta um modelo de gerenciamento de direitos digitais inspirado em blockchain que, além de proteger os direitos do autor, também garante a unicidade, rastreabilidade, confiabilidade e segurança de exemplares digitais. Este modelo permite que usuários possam revender ou emprestar arquivos digitais sem ferir os direitos autorais, e apresenta-se como uma solução para que bibliotecas possam gerenciar o empréstimo de arquivos digitais. Por fim, uma aplicação foi desenvolvida para provar o conceito do modelo e um comparativo com outros gerenciadores de direitos digitais é apresentado.*

1. INTRODUÇÃO

Garantir os direitos autorais de uma obra distribuída digitalmente é uma tarefa complexa para editoras, distribuidoras ou autores. Diferentemente de um livro físico, um arquivo digital pode ser compartilhado múltiplas vezes a partir de um único exemplar. Com tal facilidade e com a prática da pirataria destes conteúdos, toda uma cadeia produtiva acaba por ser prejudicada. Além disso, a inexistência de um projeto de aquisição específico para obras digitais é um fator que prejudica a expansão do setor e seu uso na sociedade, inclusive nas bibliotecas. Esse fator contribui diretamente para os baixos investimentos na compra de livros digitais, custos elevados para aquisição, demora nas entregas e, consequentemente, insatisfação dos clientes [MARTINS 2016].

Compreende-se, ainda, várias incertezas que abarcam os bibliotecários/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? [MARTINS 2016].

Para contornar esses problemas, 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 *Digital Rights Management* (DRM) próprios que disponibilizam o conteúdo apenas para quem possui permissão para consumi-lo. Porém, a utilização dessa tecnologia tem sido muito debatida nas comunidades espalhadas pela internet. Isso porque, 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 [IANZEN et al. 2013].

Este artigo apresenta um modelo de empréstimo digital, inspirado em Blockchain, para possibilitar que as transações sejam realizadas entre os usuários e validadas através de um mediador, garantindo a integridade e unicidade do objeto intelectual. Este artigo está dividido em: Seção 2, onde são apresentados alguns conceitos básicos para o entendimento do artigo; Seção 3, onde são apresentadas as garantias, características e operações do modelo proposto; Seção 4 onde é apresentada uma prova de conceito; e Seção 5 onde é apresentada uma comparação com alguns sistemas DRM e possíveis trabalhos futuros.

2. REVISÃO BIBLIOGRÁFICA

Nesta seção são apresentados alguns conceitos utilizados no artigo.

2.1. Blockchain

Blockchain é uma tecnologia que tem sido difundida e amplamente pesquisada por desenvolvedores. Tendo sua origem em 2008, o uso dessa tecnologia se tornou evidente principalmente com o destaque da criptomoeda Bitcoin [SANTOS et al. 2017]. Esta tecnologia utiliza-se da arquitetura peer-to-peer (P2P) para que as transações sejam feitas de forma descentralizada; consistindo em uma cadeia de blocos ordenados de forma sequencial e cronológica, por meio da qual o primeiro bloco é chamado de “bloco gênese” e os demais blocos subsequentes possuem um *digest* de seu bloco anterior. Sendo assim, o alinhamento dos blocos de forma cronológica faz com que uma transação não possa ser alterada com antecedência sem alterar seu bloco e todos os blocos posteriores [SANTOS et al. 2017] [ARAÚJO and SILVA 2017] [RODRIGUES 2017].

2.2. Hash

Hash é a função unidirecional que recebe uma entrada de dados de qualquer tamanho e produz uma saída (*digest*) de tamanho fixo, resultando em uma

identificação única para cada transação. O SHA256 é a função hash utilizada no Blockchain - gerando uma saída fixa de 256 bits [RODRIGUES 2017].

2.3. Digital Rights Management

Digital Rights Management (DRM) são sistemas de gerenciamento dos direitos digitais, cujo objetivo é prevenir o uso indevido de determinados arquivos eletrônicos, além de poder definir a autorização de acesso de um arquivo em diferentes dispositivos e/ou diferentes pessoas simultaneamente [IANZEN et al. 2013].

No caso de *e-books*, os sistemas DRM aplicam restrições de cópia, distribuição e acesso ao conteúdo digital; devido a necessidade de proteger o conteúdo adquirido pelo leitor. Essa necessidade engloba um conjunto de ações que devem ser planejadas e programadas de modo a abranger as questões técnicas comportamentais e jurídicas, visando os princípios de confidencialidade, autenticidade, integridade e disponibilidade das informações [IANZEN et al. 2013].

3. MODELO PROPOSTO

A falta de consenso entre editores e bibliotecários sobre comercialização e/ou empréstimo de e-books e as limitações impostas nos negócios, no que tange a garantia do direito autoral, provocam barreiras ao acesso à informação e instabilidade na forma de gerência desses conteúdos digitais, inibindo a expansão e a democratização desse suporte informacional na sociedade [MARTINS 2016]. Nesta seção apresentamos uma proposta de processo de empréstimo digital inspirado na tecnologia *Blockchain* para preservar os direitos autorais e possibilitar a unicidade e rastreabilidade de arquivos digitais, tornando o processo gerenciável, transparente e seguro.

Dessa forma, o modelo de empréstimo digital proposto, representado na Figura 1, está inspirado em três categorias de membros envolvidos no processo, sendo eles: *Controlador*, *Mediador* e *Usuário*. Cada um destes possui uma atribuição bem definida no processo.

Controlador: Autoridade responsável pelo controle de acesso, validação e garantia da identidade dos *Usuários* e *Mediadores* no sistema.

Mediador: Entidade portadora do direito de cópia (*copyright*), responsável por: incluir os arquivos digitais; validar, registrar e armazenar as informações sobre as atividades de transferência ou empréstimo; confirmar a identidade do *Usuário* junto ao *Controlador*. Esta entidade pode ser um autor, uma editora ou uma distribuidora.

Usuário: Entidade cadastrada no sistema que pode acessar ou transferir algum arquivo digital já existente no sistema. Esta entidade pode ser um leitor, uma biblioteca ou uma livraria.

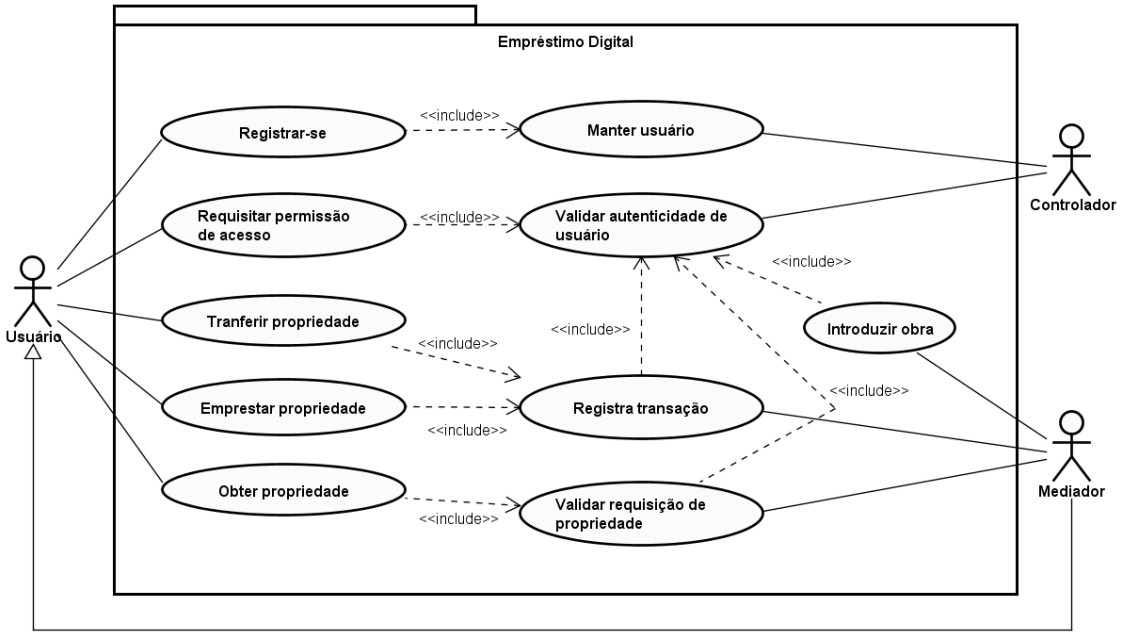


Figura 1. Visão geral do modelo proposto

3.1. Características

As características do modelo proposto são: *Inclusão*, *Transferência* e *Acesso*, conforme descritas abaixo:

Inclusão: Qualquer *Mediador*, devidamente reconhecido pelo *Controlador*, possui permissão para transferir conteúdo para a plataforma, esse conteúdo é devidamente registrado no *livro razão* e armazenado para futuro acesso do *Usuário*.

Transferência: Qualquer *Usuário* pode transferir um arquivo digital para outro *Usuário*. Esta transferência pode ser definitiva (venda) ou temporária (empréstimo). Vale ressaltar que toda transferência é feita por meio do *Mediador* para garantir que toda movimentação seja registrada. O *Mediador* valida os dados e gera um novo registro no *livro razão* para cada transação ocorrida.

Acesso: Esta característica do sistema refere-se ao acesso a um arquivo digital após a transferência de propriedade do mesmo. O *Usuário* deverá requisitar ao *Mediador* utilizando a assinatura da transferência (*digest*) que lhe foi fornecida na negociação. Assim, o sistema do *Mediador* é capaz de encontrar o arquivo gerado e fornecê-lo.

3.2. Garantias oferecidas

O modelo proposto visa garantir *Unicidade*, *Rastreabilidade*, *Confiabilidade* e *Segurança* na troca de arquivos digitais.

Unicidade: Para garantir a unicidade, todo arquivo digital recebe um cabeçalho único e é criptografado por AES (*Advanced Encryption Standard*)

com uma chave aleatória. Desta forma, cada exemplar de arquivo digital é único e sua permissão de leitura (acesso à chave criptográfica) é negociada entre *Mediador* e *Usuário* no sistema.

Rastreabilidade: O *Mediador* mantém o *livro razão*[1] onde cada registro possui sua identificação atual (*hash*) e sua identificação anterior (*old hash*), possibilitando percorrer esse encadeamento de registros, construindo um histórico de todas as transações do arquivo digital.

Confiabilidade: Uma vez que o sistema proposto está inspirado em *Blockchain* não é possível negar a transação realizada, pois todas as transações são registradas no *livro razão* e que, para burlar o conteúdo de uma transação, seria necessário alterar o *digest* de toda a cadeia de transações anteriores [RODRIGUES 2017] [ARAÚJO and SILVA 2017].

Segurança: Toda transferência ou empréstimo passa por três etapas criptográficas, conforme apresentado na Figura 2, sendo elas: 1) utiliza-se o AES e uma chave gerada por um GNPA (Gerador de Número Pseudo-Aleatório); 2) a chave aleatória é criptografada via RSA com a chave pública do *Usuário* fornecida pelo *Controlador*; 3) a chave e o arquivo digital são novamente cifrados utilizando-se AES e uma chave conhecida apenas pelo sistema, garantindo assim a segurança na transmissão do arquivo entre as partes.

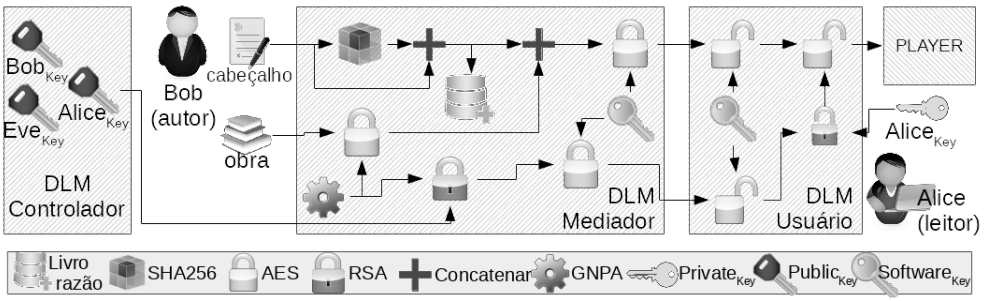


Figura 2. Diagrama do fluxo criptográfico

3.3. Detalhamento das operações

Nesta seção serão detalhadas as operações de *Transação*, *Acesso*, *Permissão* e *Leitura*, previstas neste modelo de empréstimo digital.

3.3.1. Transação

Uma transação é caracterizada pela transferência definitiva ou temporária da propriedade de um arquivo digital. O processo de transação realizada pelo *Mediador* é composta por: registro no *livro razão*; geração de uma assinatura da transação (*digest*); geração de chave criptográfica aleatória; e cifragem do

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

arquivo digital. Os passos do procedimento de transação estão descritos no Algoritmo 1. Os dados envolvidos nos registros do *livro razão* são apresentados na Tabela 1.

Algorithm 1 Procedimento de transação

function *Mediador*.transferir($arquivo, origem, destino, deadline$)
  if $Controlador.valida(origem, destino) == true$ **then**
    $head = new(arquivo.head, destino, deadline)$;
    $digest = SHA256(head)$;
    $arquivo.head = head + digest$;
    $Livro_{razao}.add(arquivo.head)$;
    $keyRandom = random.new()$;
    $keyDoc = RSA.encrypt(keyRandom, Controlador.getRSA_{public}(destino))$;
    $Storage.set(digest, AES.encrypt(arquivo, keyRandom), keyDoc)$;
    return $digest$;
  return $null$;

Para a efetivação de uma transação o *Usuário* deve requisitar ao *Mediador* a transferência, informando o destinatário e o tempo de duração. O *Mediador* valida os *Usuários* envolvidos, junto ao *Controlador*; gera os dados do novo cabeçalho, gerando uma assinatura com todos os dados do cabeçalho; criptografa o arquivo com uma chave aleatória; criptografa a chave aleatória para que somente o destinatário tenha acesso; registra a transação no livro razão; por fim retorna o código da transação. O *Usuário* deve enviar o código da transação para que o destinatário possa requisitar o documento junto ao *Mediador*.

Tabela 1. Descrição dos campos armazenados no *livro razão*

Campo	Descrição
hash	Identificação única
owner	Dono do arquivo
oldHash	Hash da transação anterior
time	Validade de empréstimo
date	Data/Hora da realização da transação
user	Pessoa que possui direito de acesso

Tabela 2. Exemplo de 1ª transação armazenada no *livro razão*

Campo	Valor
hash	#01
owner	@proprietario
oldHash	null
time	null
date	99/99/9999-99:99:99
user	@proprietario

Vale destacar que a primeira transação realizada (apresentada na Tabela 2) é sempre por tempo indeterminado, sendo ela de propriedade e acessível ao *Usuário* que adquiriu o arquivo diretamente do *Mediador*. O processo das demais transações utilizará o mesmo padrão e terá a assinatura anterior em seus registros, um exemplo de registro de transações no livro razão pode ser observado na Tabela 3.

Tabela 3. Exemplo do registro de transações do arquivo no *livro razão*

Ação	Revenda	Empréstimo	Empréstimo
hash	#02	#03	#04
owner	@proprietario2	@proprietario2	@proprietario2
oldHash	#01	#02	#03
time	null	99/99/9999-99:99:99	99/99/9999-99:99:99
date	99/99/9999-99:99:99	99/99/9999-99:99:99	99/99/9999-99:99:99
user	@proprietario2	@usuarioX	@usuarioY

3.3.2. Acesso

O acesso ao arquivo digital deve ser solicitado pelo *Usuário* destinatário ao *Mediador*, através da informação do código de transação anteriormente efetivada (*digest*). Este por sua vez enviará o arquivo caso: as credenciais do requisitante sejam validadas pelo *Controlador*; o requisitante seja o *Usuário* com permissão de acesso e o empréstimo esteja dentro do prazo válido, conforme registro no *livro razão*. O procedimento de acesso está descrito no Algoritmo 2.

Algorithm 2 Procedimento de acesso

1: **function** *Mediador*.acessarArquivo($usuario, digest$)
2: **if** $Controlador.valida(usuario) == true$ **then**
3: $arquivo = Storage.get(digest)$;
4: $head = arquivo.head$;
5: **if** $((head.time > Date.now) OR (head.time == null))$ $AND(head.user == usuario)$ **then**
6: **return** $arquivo$;
7: **return** $null$;

3.3.3. Permissão

A permissão de leitura é baseada na obtenção da chave aleatória gerada na encriptação do arquivo digital. A requisição da chave é feita pelo *Usuário*, informando ao *Mediador* o código da transação (*digest*), este por sua vez deve: validar o usuário junto ao *Controlador*; verificar a ser o *Usuário* possui permissão de leitura no *livro razão*; e verificar se está dentro do tempo limite para acesso. No Algoritmo 3 está descrito o procedimento de obtenção da chave aleatória.

3.3.4. Leitura

Uma vez que o *Usuário* está de posse da chave aleatória, o software leitor valida o utilizador e o tempo de expiração através do cabeçalho do arquivo. Caso

Algorithm 3 Procedimento de solicitação de chave

```
1: function Mediador.acessarChave(usuario, digest)
2:     if Controlador.valida(usuario) == true then
3:         arquivo = Storage.get(digest);
4:         head = arquivo.head;
5:         if ((head.time > Date.now)OR(head.time == null))
   AND(head.user == usuario) then
6:             return Storage.getKey(digest);
7:     return null;
```

o tempo esteja em vigência a chave aleatória é decriptada utilizando a chave RSA privada do *Usuário* e então utilizada para decriptar via AES o arquivo digital que é exibido. Caso o tempo de vigência esteja expirado o software leitor destrói a chave e o arquivo digital. O funcionamento do software leitor está descrito no Algoritmo 4.

Algorithm 4 Procedimento de leitura do arquivo

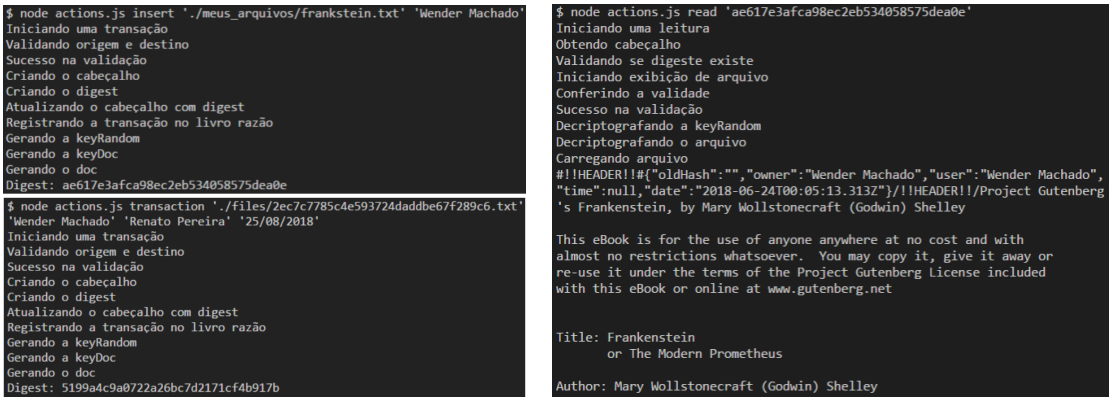
```
1: procedure Usuario.lerArquivo(arquivo, privateKey_RSA)
2:     head = arquivo.head;
3:     if Storage.keyExists(head.digest) == false then
4:         Storage.setKey(digest, Mediador.acessarChave(usuario, digest));
5:     ExibirArquivo(arquivo, privateKey_RSA);
6: procedure Usuario.exibirArquivo(arquivo, privateKey_RSA)
7:     head = arquivo.head;
8:     if ((head.time > Date.now)OR(head.time == null)) then
9:         keyRandom = RSA.decrypt(Storage.getKey(head.digest), privateKey_RSA);
10:        print(AES.decrypt(arquivo,keyRandom));
11:    else
12:        destroy(arquivo);
13:        Storage.destroy(digest);
```

4. IMPLEMENTAÇÃO DO MODELO PROPOSTO

Para provar o conceito do modelo idealizado foi construída uma aplicação em Node.js e o seu código fonte está disponibilizado no GitLab[2] a qual possibilita a demonstração do funcionamento das transações e suas questões de segurança. Foram pré-cadastradas algumas contas fictícias e utilizadas obras de domínio público, retiradas do site Projeto Gutenberg[3].

Um exemplo de primeira transação (venda) e um exemplo de empréstimo é apresentado na Figura 3(a). Um exemplo de leitura de arquivo protegido pelo modelo proposto é apresentado na Figura 3(b). O manual para uso do software construído é apresentado na Figura 4.

[2] https://gitlab.com/si-cefet-nf/dlm
[3] http://www.gutenberg.org/



(a) Exemplo de primeira transação e empréstimo

(b) Exemplo de leitura de arquivo

Figura 3. Exemplos de uso do software implementado

```
# Primeira transação (venda):
$ node actions.js insert [ARQUIVO] [DESTINATARIO]

# Transferência de propriedade (revenda):
$ node actions.js transaction [ARQUIVO] [DESTINATARIO]

# Transferência de propriedade com tempo determinado (empréstimo):
$ node actions.js transaction [ARQUIVO] [DESTINATARIO] [DATA_VENCIMENTO]

# Abertura de arquivo:
$ node actions.js read [HASH]
```

Figura 4. Manual do sistema implementado

5. DISCUSSÃO

Este artigo apresentou uma metodologia para empréstimo digital que garante *Unicidade*, *Rastreabilidade*, *Confiabilidade* e *Segurança*, possibilitando bibliotecas, livrarias e leitores trocarem conteúdos digitais entre si de forma segura, transparente e, principalmente, garantindo os diretos autorais de editoras e/ou autores. Devido a rastreabilidade das transações de empréstimo e/ou venda e a centralização na figura do *Mediador*, editoras e/ou autores poderão minerar dados no *livro razão* de forma a construir uma base estatística mais precisa em relação as suas obras, possibilitando ações de marketing melhor definidas e consequentemente o crescimento em suas vendas.

Na Tabela 4 é apresentado um comparativo entre o modelo proposto e os DRMs utilizados pelas plataformas Play Livros[4], Kindle[5] e iBooks[6]. Podemos destacar algumas vantagens do modelo proposto, sendo elas: a) Os direitos autorais e o processo de transferência de compra são garantidos por todos. Porém, apenas no DLM um usuário poderá comprar um livro de outro

[4] https://play.google.com/books/intl/pt-BR/privacy.html

[5] https://www.amazon.com.br/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=201283910

[6] https://support.apple.com/pt-br/ht201478

usuário (proprietário); b) A transferência de propriedade cria uma economia de arquivos digitais, possibilitando a existência de sebos digitais; c) O empréstimo entre usuários soluciona o problema da expansão no uso dos e-books por bibliotecas públicas, conforme apresentado por [MARTINS 2016]; d) Implementa a tecnologia Blockchain em suas transações, garantindo a rastreabilidade e transparência no processo de empréstimo digital; e) devolve ao leitor a sensação de posse, uma vez que o mesmo pode emprestar, doar ou revender, conforme apontado por [IANZEN et al. 2013].

Futuramente outros trabalhos poderão desenvolver aplicações completas integradas com leitores que possibilitem a troca e leitura de e-books. Novas garantias e funcionalidades poderão ser idealizadas, tais como a assinatura do livro razão por outros *Mediadores* ou pelo *Controlador* para garantir a irretratabilidade das transações.

Tabela 4. Comparativo entre alguns DRM 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

Referências

ARAÚJO, H. P. and SILVA, R. B. A. R. (2017). A Tecnologia Digital Blockchain: Análise Evolutiva e Pragmática. *Revista Fatec Zona Sul - REFAS*, v. 3(n. 4).

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.

MARTINS, R. D. (2016). Obstáculos para expansão do uso dos e-books na sociedade brasileira. *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação*, v. 14(n. 2):p. 279–297.

RODRIGUES, C. K. d. S. (2017). Uma análise simples de eficiência e segurança da Tecnologia Blockchain. *Revista de Sistemas e Computação*, v. 7(n. 2):p. 147–162.

SANTOS, S. C. D., FERREIRA, J. E., and PINTO, F. G. C. (2017). Estudo de Mapeamento Sistemático sobre as Tendências e Desafios do Blockchain. *GESTÃO.Org - Revista Eletrônica de Gestão Organizacional*, v. 15(n. 2):p. 108–117.