Gestão de Direitos Digitais através de Contratos Inteligentes

Henrique Júnior de Souza Oliveira, 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@gmail.com, nilson.lazarin@cefet-rj.br

Abstract. *DRM systems impose to the user several restrictions and limiting on the use of e-books. Smart Contracts have great potential for application in DRM systems in order to guarantee copyright, without prejudice to the consumers freedom. This paper shows a model of DRM over Smart Contracts allow selling or exchanging a digital file between users of the a same blockchain. The proposed model intends to align the idea of the lending or selling digital files and the concept of automatic management of copyrights using Smart Contracts.*

Resumo. *Smart Contracts se apresentam com grande potencial de aplicação em sistemas de DRM de modo a garantir os direitos da obra sem prejudicar a liberdade do usuário, uma vez que, os atuais sistemas tem se efetivado como mecanismos de controle e restrição, limitando a sensação de posse de consumidores de obras digitais. Este artigo apresenta um modelo de gerenciamento de direitos autorais através de Smart Contracts como possível solução ao desafio de garantir os direitos do autor sem ferir a liberdade de uso do usuário que a adquiriu. 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.*

1. Introdução

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. 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. Garantir os direitos autorais de uma obra distribuída digitalmente ainda tem sido uma tarefa complexa para editoras, distribuidoras ou autores [OLIVEIRA et al. 2019]. E, portanto, como as discussões sobre o uso das obras protegidas por direitos autorais e a intervenção jurídica na Internet 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 *Smart Contracts*, 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. Diferentemente de tecnologias convencionais de 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].

Este artigo 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 da obra, podendo realizar empréstimos e/ou revendas desses arquivos através da Internet.

2. Revisão Bibliográfica

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 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. A 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. O monitoramento busca enviar relatórios automatizados acerca de atividades do usuário no consumo daquele bem. E por fim, o 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].

A *Blockchain* é uma tecnologia que utiliza-se da arquitetura peer-to-peer (P2P) para que 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. 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].

Os *Smart Contracts*, surgiram como uma implementação promissora da tecnologia Blockchain. Porém, em 1994, o idealizador Nick Szabo 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 *Smart Contracts* são contratos digitais que permitem termos contingentes em consenso descentralizado, normalmente à 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 pôde 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 *Smart Contracts* se apresenta com grande potencial de aplicação em sistemas de DRM de modo a garantir os direitos da obra sem prejudicar a liberdade do usuário [FUJIMURA et al. 2015].

3. Trabalhos Relacionados

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.

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 não 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 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 no servidor para garantir a unicidade, rastreabilidade, confiabilidade e segurança do arquivo digital.

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 *Smart Contracts*. 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 *Smart Contract*) 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 *Smart Contracts*. 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 da obra, possibilitando a unicidade e a rastreabilidade de arquivos digitais, tornando o processo gerenciável, transparente e seguro.

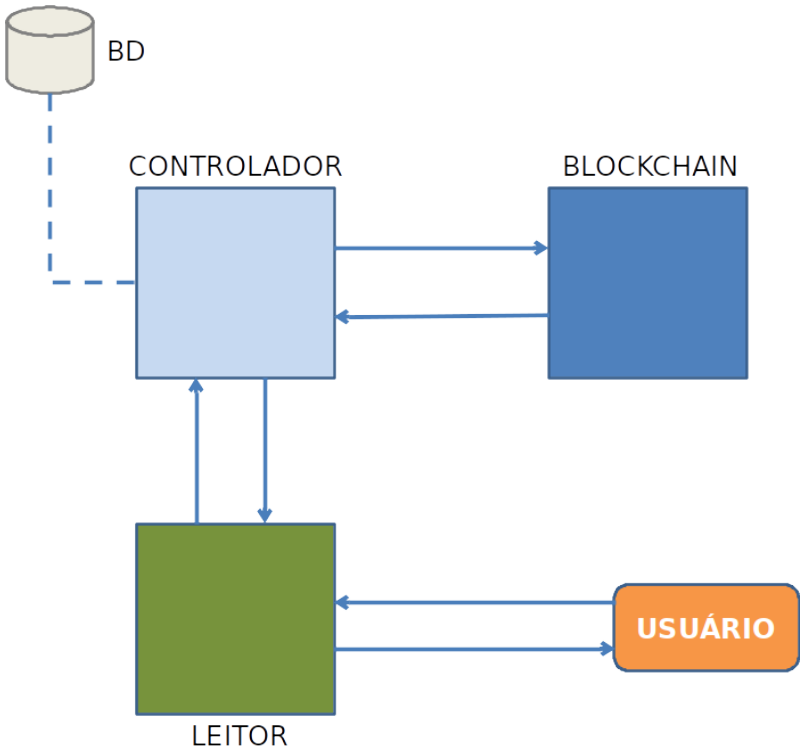


Figura 1. Modelo Proposto

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 1. 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 a obra posteriormente; gerar o hash do conteúdo da obra (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 da obra e da carteira do usuário; validar as permissões do usuário, junto ao Controlador; e decifrar o arquivo digital recebido do Controlador.
- A Blockchain é responsável por armazenar os registros das obras transacionadas 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 válida 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 obra e a identificação das carteiras de origem e destino. 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 2.

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 2. Campos registrados na Blockchain

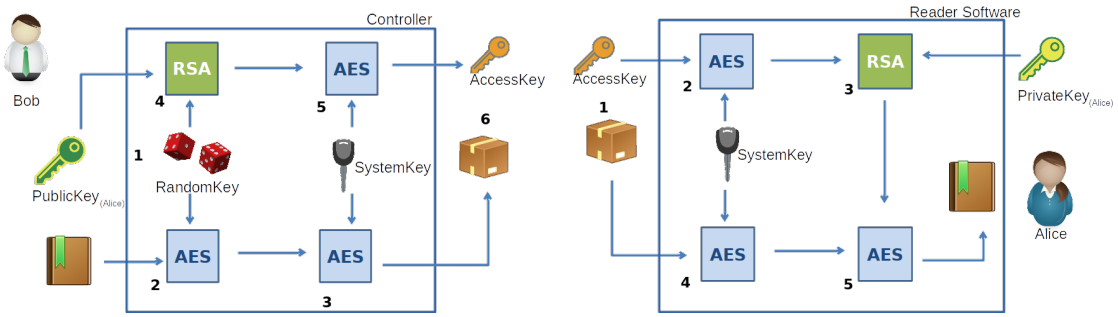
Vale destacar que o Contrato Inteligente é imprescindível para que os registros de licença dos arquivos digitais sejam salvos na Blockchain. Sendo assim, antes de qualquer transação no modelo, necessitamos fazer o upload do contrato para a Blockchain em uma transação do tipo *"contract"*, registrando 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 divido 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 3 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 da Figura 2 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.



(a) Cifragem no Controlador (b) Decifragem no Leitor

Figura 3. 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[1] EVM (*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 4 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[2] para fazer o upload do *Smart Contract* para o Ganache EVM. O *Smart Contract* foi descrito em Solidity[3], uma linguagem de programação de alto nível, orientada a contratos. Por fim, para que o membro Controlador pudesse se comunicar a Blockchain, foi necessário utilizar a API Ethereum JavaScript Web3.js[4], que permite integração com um nó Ethereum local ou remoto, usando conexões HTTP ou IPC.

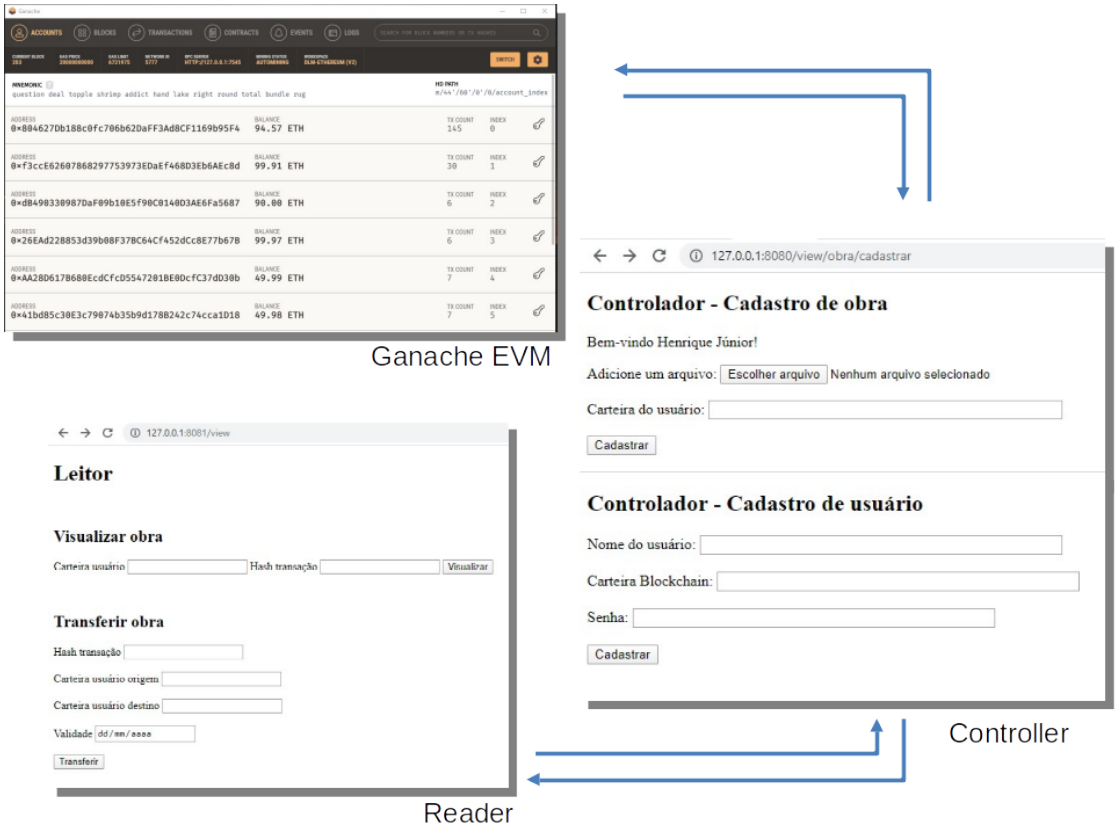


Figura 4. Implementação

[1]https://www.trufflesuite.com/ganache
[2]https://www.trufflesuite.com/truffle
[3]https://solidity.readthedocs.io/en/v0.6.4/
[4]https://web3js.readthedocs.io/en/v1.2.6/

5. Conclusão

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 determinando arquivo digital [OLIVEIRA et al. 2019] [OLIVEIRA 2019]. Entretanto, o surgimento dos *Smart Contracts* se apresenta com grande potencial de aplicação em sistemas de DRM de modo a garantir os direitos da obra sem prejudicar a liberdade do usuário [FUJIMURA et al. 2015].

O objetivo deste artigo é apresentar um modelo de empréstimo e/ou revenda de arquivos digitais utilizando-se dessas tecnologias emergentes no mercado e que se colocam como grandes promissoras nesse desafio que é garantir os direitos autorais da obra sem ferir a liberdade de uso do usuário que a adquiriu. 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, consequentemente, 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 obras diminuiria, devido ao menor esforço estabelecido pela tecnologia Blockchain, além de possibilitar a autores/editoras identificar, através da rastreabilidade, como determinada obra tem sido transacionada na Internet, permitindo tirar conclusões para tomada de decisões a nível de negócio.

Referências

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.

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)*.

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

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.