II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I

T255
Tecnologias Disruptivas, Direito e Proteção de Dados - I [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Lorena Muniz e Castro Lage; Yuri Nathan da Costa Lannes; Marco Antônio Sousa Alves. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia
ISBN: 978-65-5648-272-9
Modo de acesso: www.conpedi.org.br
Tema: Um olhar do Direito sobre a Tecnologia

1. Direito. 2. Inteligência Artificial. 3. Tecnologia. II. Congresso Internacional de Direito e Inteligência Artificial (1:2021 : Belo Horizonte, MG).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I

Apresentação

Renovando o compromisso assumido com os pesquisadores de Direito e tecnologia do Brasil, é com grande satisfação que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 12 livros produzidos a partir dos Grupos de Trabalho do II Congresso Internacional de Direito e Inteligência Artificial (II CIDIA). As discussões ocorreram em ambiente virtual ao longo dos dias 27 e 28 de maio de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área em cinco painéis temáticos e o SKEMA Dialogue, além de 354 inscritos no total. Continuamos a promover aquele que é, pelo segundo ano, o maior evento científico de Direito e Tecnologia do Brasil.

Trata-se de coletânea composta pelos 255 trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito Grupos de Trabalho originais, diante da grande demanda, se transformaram em doze e contaram com a participação de pesquisadores de vinte e um Estados da federação brasileira e do Distrito Federal. São cerca de 1.700 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 36 proeminentes professoras e professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, mais uma vez, o grande legado do evento.

Neste norte, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais. Fomentou-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários

campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Já está em funcionamento o projeto Nanodegrees, um conjunto de cursos práticos e avançados, de curta duração, acessíveis aos estudantes tanto de graduação, quanto de pós-graduação. Em breve, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área. A SKEMA estrutura, ainda, um grupo de pesquisa em Direito e Inteligência Artificial e planeja o lançamento de um periódico científico sobre o tema.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 09 de junho de 2021.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School

A SEGURIDADE NO FUNCIONAMENTO DA BLOCKCHAIN E SEU PAPEL NA EXECUÇÃO DOS SMART CONTRACTS.

SECURITY IN THE FUNCTIONING OF THE BLOCKCHAIN AND ITS PARTICIPATION IN THE EXECUTION OF SMART CONTRACTS.

Mariana Rodrigues Coelho de Souza

Resumo

O presente trabalho expõe de forma didática o funcionamento de um sistema descentralizado e distribuído como a Blockchain, desde sua formação .Serão explorados conceitos base como elementos de formação de um bloco na cadeia, até sua inserção na referida, e a garantia de seguridade das informações inseridas por meio do Hash e mineração. Bem como explanado acerca dos sistemas de chaves, criptografia e assinatura digital Por fim, apresenta-se a utilidade de todo este sistema na automatização dos SmartContracts.

Palavras-chave: Blockchain, Smart contracts, Seguridade, Criptografia

Abstract/Resumen/Résumé

The following work expounds in a didactic way the functioning of a decentralized and distributed as a blockchain system since its formation.In this bias, base concepts will be explored as elements from a block in the chain until its insertion in the afore mentioned and the security warranty from the inserted information through hash and mining.It will also be displayed about the key systems, cryptography and digital signature. Eventually it is presented all this system utility in the Smart Contracts automatization.

Keywords/Palabras-claves/Mots-clés: Blockchain, Smart contracts, Security, Cryptography

1. Introdução

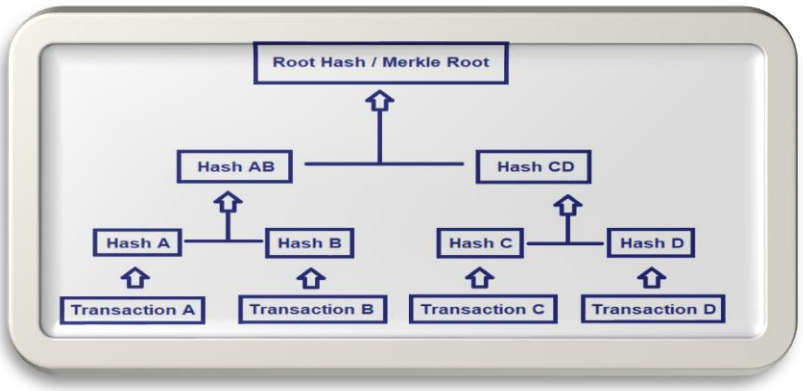
Em termos práticos, a *Blockchain é* um grande "livro de fatos" o qual o registro é feito e verificado virtualmente pelos chamados mineradores. Em sua tradução literal significa corrente ou cadeia de blocos. Estes blocos armazenam informações, transações, ou qualquer dado que nele seja inserido e validado. A cadeia apenas caminha adiante, melhor dizendo, a informação, uma vez inserida não pode ser alterada, isso se deve a própria segurança e confiabilidade do sistema, que conta com uma rede de computadores em constante mineração.

Além disso, como o registro é feito na rede mundial de computadores, cada computador pertencente à referida rede mantém uma cópia da *Blockchain*, assim, com uma simples comparação, é possível, de forma eficaz, identificar se as informações inseridas nos blocos são compatíveis entre si, tornando qualquer tentativa de fraude obsoleta e de fácil identificação. Essa facilidade se deve ao fato de o sistema ser descentralizado e distribuído e, por consequência, depender de poder computacional para verificação. A grande gama de computadores envolvidos na rede, que transacionam, mineram, verificam e armazenam informações é o chamado poder computacional.

2. Estrutura de um Bloco e sua inserção na corrente

A *Blockchain* é comparada a um grande livro de fatos, um verdadeiro banco de dados, progressivo, são necessários vários blocos para formar uma corrente. Os referidos possuem estruturas específicas que garantem sua identidade e a correta ligação com os demais blocos. Cada um deles possui o *"Block Size"* que é o tamanho do bloco em bytes, o *"Transaction Conter"*, campo que que informa quantas transações o bloco tem, os campos que contém as transações em si mesmas e o *"Blockheader"* que é o cabeçalho, o qual possui seis espaços internos, quais sejam, *"Version",* que designa o número do *software* e atualizações, *"Previous Bock Hash"* que é preenchido com o número do "*Hash"* do bloco anterior, *" Root Hash"* o qual indica o *Hash* resultante das transações realizadas no bloco em questão*, " Timestump"* que mostra a data e hora aproximada da criação do bloco, *"Difficult Target"* que simboliza a dificuldade do algoritmo empregado naquele bloco (quanto mais complexa a transação, mais difícil o desafio matemático e mais remuneração o minerador recebe) e *"Nonce"* que é um Número aleatório que auxilia a revelar o algoritmo nele inserido.

Importa ressaltar que o "*Root Hash"* é obtido pelo o que se chama de "*Merkle Trees"*, a qual não é nada mais que o caminho de transações realizadas e seus respectivos "*Hashes"* resultantes, combinados, utilizando a criptografia, que originam o "*Root Hash"*.



[1]

Pela imagem alhures possível notar que cada transação possui um código, um *"Hash",* o qual será combinado com o resultante de outra transação a fim de se formar um segundo o qual, ainda será combinado com o código resultante de outras transações objetivando a formação de um *"Hash"* final que representa todas as transações inseridas no bloco.

Dessa maneira possível perceber que, dentro de um bloco, todas as informações estão interligadas e são interdependentes, nesta senda, uma mínima alteração em uma transação, alteraria o *"Hash"* da referida, logo, adulterada estaria a "*Merkle Tree"*, o que modificaria também o "*Root Hash"* resultando em um *"Block Hash"* totalmente distinto e, consequentemente, afetaria a própria existência do bloco na corrente, haja vista que novo "*Hash"* resultante, não seria o mesmo designado no espaço do "*Previus Block Hash*" do bloco posterior. Enfim, o efeito em cascata seria catastrófico. Uma pequena alteração, portanto, ricocheteia em todo bloco, e modifica toda a corrente de blocos posteriores.

3. Elementos de Segurabilidade e verificação

O *"Hash"* é um fator responsável pela seguridade no sistema *Blockchain*. É uma função utilizada a fim de se representar dados inseridos, é o resultado do desafio lógico matemático resolvido através do processo de mineração. O referido processo também é responsável por validar informações e transações inseridas. Como ele representa a informação, se esta for alterada de alguma maneira, a função resultaria em um *"Hash"* totalmente distinto, conforme já exposto, o que seria identificado pela rede facilmente, haja vista que a *Blockchain* é um sistema distribuído e descentralizado. De mais a mais é praticamente impossível um usuário acessar uma cadeia de blocos, alterar apenas uma informação em seu interior, que todos os posteriores são interligados a este e verificados.

[1] Retirado de https://medium.com/@marcosgabbardo/merkle-tree-no-blockchain-170b490b42b3

Assim, chega-se ao ponto: como verificar uma informação/transação inserida no sistema e garantir que a referida é verdadeira? Como garantir que há uma validação coerente das informações ao liga-las à cadeia? Uma maneira popular é a chamada de Mineração, muito utilizada na realização de transações com uma criptomoeda chamada *Bitcoin* ou no Sistema *Ethereum* por meio da *Blockchain*.

Em primeiro lugar, cumpre ressaltar que o processo não é humano. Os "nós" são computadores participantes da rede e são responsáveis por este trabalho. Um minerador nada mais é que um computador configurado para tal função. Os computadores mineradores registram na *Blockchain*, dessa forma concorrem entre si a fim de resolverem um desafio lógico matemático que lhes permitem verificar e adicionar a informação na cadeia, assim, a máquina que resolver a função de forma mais rápida, terá permissão para adicionar a transação à corrente e, por consequência será remunerada em criptomoeda.

Essa "disputa" pode ser didaticamente dividia em duas etapas, supondo uma relação entre dois sujeitos "A" e "B" em que haja uma transação financeira em que o primeiro transfere para o segundo 1BitCoin: na primeira etapa os mineradores irão verificar e validar a relação existente entre os dois sujeitos, verificar se A possui realmente a quantidade de dinheiro pactuada. E como fazem isso? O sistema *Blockchain* é público, permitindo consulta por qualquer indivíduo, além disso, guarda um histórico de todos os acontecimentos, sendo possível realizar um *"Audit Trail",* uma trilha de auditoria a qual irá permitir verificar todas as transações e informações já compartilhadas por 'A" desde o momento que ingressou *na BlackChain*, desta maneira, possível verificar se "A" em algum momento anterior inseriu em sua *Wallet* (carteira virtual) alguma quantidade "x" de criptomoeda sendo essa informação já verificada e validada pelo sistema em algum momento anterior.

Neste diapasão os mineradores conferirão se "A" tem o saldo necessário e se a verificação for positiva, inicia-se a segunda etapa: Os mineradores iniciam uma competição entre si a fim de encontrar um código único e especial, resolvendo um desafio matemático o qual utiliza a lógica computacional, que, ao final fornecerá o código, o *"Hash"* o qual representará resumidamente a informação inserida e permitirá adicionar a transação entre A e B ao sistema. Não existe fórmula pronta, é um número aleatório, dessa forma o minerador que encontrar primeiro esse código comunicará a todos os outros do sistema, os quais poderão conferir e verificar a veracidade da fórmula encontrada, permitindo-o, por fim, adicionar a transação a cadeia e nas cópias em que cada um possui. Lembrando que todo esse processo é feito por maquinas, não há subjetividade, apenas criptografia e cálculos.

Essa competição entre os mineradores (processo de mineração) é um dos fatores que mantem a integridade do sistema, haja vista que, como já relatado, ao final, aquele que encontrar o código correto, recebe uma remuneração por isso. Quanto mais complexa a transação, maior a competição, logo, maior remuneração oferecida.

Ainda em termos de segurança, existem três tipos de sistemas base: o centralizado o decentralizado e o distribuído. No primeiro existe apenas uma autoridade controladora e verificadora dos dados, relações e transações entre os sujeitos, como exemplo, considera-se que cada instituição bancária constitui um sistema centralizado o qual tem o papel de armazenar dados pessoais e verificar transações de seus clientes, dessa maneira, quando há uma transação bancária simples (TED ou DOC), as referidas são intermediadas por esse ente.

Na mesma linha, provedores de internet também são um exemplo útil. É um único sistema central que controla e distribui toda a rede de cabos para internet, presta serviços de manutenção, internet, "banda larga", ligações, televisão, etc. Nesse sentido, todas a transações e serviços dependem do correto funcionamento da matriz.

Cumpre ressaltar que, em ambos os casos, o problema se instaura quando essa única autoridade controladora sofre com alguma pane geral como a queda no sistema ou um ataque cibernético realizado por *Hackers*, deixando todos os seus dependentes também desamparados

De outro lado, em um sistema descentralizado existem vários pontos de controle, o que torna toda a situação mais democrática, assim, os "nós" (membros participantes da rede) centrais são responsáveis por exemplo, pelo armazenamento de dados de seus dependentes, deste modo, se um deles falhar, os demais ainda podem continuar trabalhando normalmente, sendo possibilitado ainda que seja feitas novas conexões.

O sistema distribuído caminha nesse mesmo sentido, e ainda oferece mais: em um sistema distribuído, todos os "nós" (computadores inseridos na rede) processam todas as informações, não há "pontos de autoridade". Assim, se um falhar, todos os outros possuem a mesma parte do arquivo que este, o que torna muito mais fácil a recuperação, verificação e validação de arquivos e transações já que cada "nó" possui uma cópia ou parte do arquivo quando a informação é solicitada, assim, todos os fragmentos da referida são condensadas e exibidas. Importa ressaltar que esse processo não é visível, tudo ocorre na rede e depende de criptografia.

O melhor exemplo dos dois últimos sistemas supracitados é a Blockchain; nela não há apenas uma entidade controladora e as informações inseridas estão dispersas por toda cadeia, possibilitando que cada computador conectado na rede, verifique, valide os dados ali inseridos e tenha uma cópia atualizada das alterações e validações que já ocorreram. Logo, "poder

computacional" é o nome que se dá a toda essa rede de milhares de computadores que trabalham em uníssono, realizando, por exemplo, a mineração, validando e verificando informações, obtendo cópias das cadeias formadas. Assim, quanto mais computadores trabalhando na rede, mais difícil é alteração das informações inseridas.

Neste caminho a dinâmica da Blockchain nos permite chegar uma consequência lógica: uma baixa significativa nas tentativas de fraude. Deste modo, imaginemos uma situação hipotética em que um indivíduo "Z" queira invadir a rede e alterar apenas um dado no interior de um bloco da corrente: este sujeito teria que ter sozinho poder computacional suficiente para invadir no bloco em questão e todas as suas cópias distribuídas, além de ter que modificar ainda as informações dos blocos posteriores relacionados, haja vista que estes possuem o número de *Hash* do bloco anterior, conforme já exposto.

Assim, modificar informações que toda a rede afirma ser verdadeira e verificada seria realizar o chamado "Ataque 51%": esse indivíduo teria que ter sozinho um poder computacional de pelo menos 51% da rede, ou seja, controlar mais da metade dos computadores responsáveis pelos processos de mineração, hackear um por um para alterar a verdade ali inserida, transfigurar uma informação falsa, tornando-a verdadeira, o que é próximo de impossível de ocorrer

De maneira a reforçar a segurança, as informações também são criptografadas utilizando um sistema de chaves.Em uma ótica genérica, um sistema simétrico é aquele em que a mesma chave é usada pra criptografar e decodificar uma informação/transaçãoPor outro lado, a criptografia assimétrica utiliza um par chaves para proteção de dados, o que garante maior confiabilidade ao sistema. Assim, algoritmo de criptografia utiliza a chave pública do destinatário para criptografar a mensagem/transação e, assim que a mensagem chega, este utiliza sua chave privada para decodifica-la.

Neste caminho, sistema de chaves pública/privada constitui método de criptografia assimétrica de dados em que se utiliza as chaves do destinatário da mensagem e se baseia em uma função chamada "Função de Direção Única", a qual é fácil em uma direção e difícil na outra, melhor dizendo, fácil de realizar a criptografia haja vista que é necessária apenas a chave pública do destinatário e difícil de reverter o processo, pois, apenas quem tem a chave privada correta obtém sucesso. Chave Pública é basicamente o endereço do usuário na rede, um "login", a identificação do indivíduo e pode ser compartilhada com qualquer outra pessoa com a qual o indivíduo queira, por exemplo, transacionar ou trocar qualquer mensagem. Por outro lado, a chave privada, como o próprio nome já remete, é particular, pode ser usada para decodificar a mensagem recebida ou para realizar uma assinatura digital.

Assim, reforça-se que no processo de criptografia, utiliza-se o par de chaves do destinatário de modo que o remetente utiliza a chave pública (endereço) do destinatário para criptografar a mensagem e quando esta chega ao destino, este utiliza sua chave privada para decodifica-la.

Na Assinatura digital, processo também assimétrico, assim, o par chave pública/ privada é utilizado de maneira a verificar a autenticidade da mensagem enviada, isto é, se a referida não sofreu qualquer adulteração ou tentativa de frade. Diferentemente do procedimento de criptografia, utiliza-se as chaves do remetente, deste modo, este utiliza sua chave privada, aplicando-a sobre o resumo já criptografado (processo alhures) criado pelo algoritmo de Hash para realizar sua assinatura digital e, quando a mensagem chega ao destinatário, este se utiliza da chave pública do referido remente para verificar a autenticidade.

4. Os Contratos Inteligentes (*Smarts Contracts)* e sua operabilidade na *Blockchain*

É mister ressaltar que a *Blockchain* por si só conta com os dois processos trabalhado concomitante, criptografia e assinatura digital. Em termos de aplicabilidade, podemos utilizar a referida plataforma para a execução de um *Smart Contract*, tendo em vista que o referido é um conjunto de códigos, um protocolo auto executável, muito utilizado como exemplo de funcionamento da máquina de venda automática em que se insere uma quantia em dinheiro e, após verificado o valor e o produto escolhido, a própria máquina continua o processo automaticamente, executando a transação. Assim a *Blockchain* tem a função de "automatizar a função dos contratos", como bem posicionou Maria Godoy em seu artigo "*Blockchain* Aplicada aos Contratos Inteligentes: Perspectivas Empresariais e Natureza Jurídica"[2]

A sistemática dos *Smart Contracts* se dá por implementação de condições: "se ocorre X, haverá consequência Y", que estará disposta dentro do código pelo qual o contrato será regido, e este por seu próprio código associado à *Blockchain* tem natureza irretroativa.

Em um viés jurídico, ainda paira uma discussão se o *Smart Contract* é de fato um contrato, e, se assim classificado, poderá ser considerado um negócio jurídico com todos os seus elementos essenciais de existência, validade e eficácia estabelecidos pelo Código Civil de 2002 bem como as demais Normas e jurisprudências do Direito, ou um mero protocolo de execução.

De qualquer forma este instrumento tem ganhado popularidade após a maior popularidade das Criptomoedas. Como exemplo, tem-se a utilização deles em leilões

[2] **Direito Digital: Debates Contemporâneos** / Coodenação por Ana Paula M. Castro de Lima, Carmina Bezerra Hissa, Paloma Mendes Saldanha – 11Ed- São Paulo: Thomson Reuters, Brasil, 2019

eletrônicos, para verificar automaticamente a maior proposta ofertada dentro do prazo determinado, reembolsando os participantes que fizeram ofertas, realizando loterias descentralizadas.

5. Considerações Finais

Por fim o que seria mais seguro que utilizar a plataforma *Blockchain* para a rodagem dos *Smart Contracts?* Nele a utilização criptografia assimétrica de forma intrínseca o torna auto executável, e assim todas as transações após verificadas ficariam registradas nos blocos, que, por si próprios já possuem cada um, sua rede de segurança. Além disso, as informações e transações seriam constantemente verificadas antes e depois de serem inseridas na corrente pelos mineradores, em tempo real, e distribuídas no sistema, sem possibilidade de alteração fácil, a não ser por um novo protocolo estabelecido por um novo Contrato Inteligente.

Referências:

PINHEIRO, Patrícia Peck – **Direito Digital**/Patrícia Peck Pinheiro. – 7.ed. – São Paulo: Saraiva Educação, 2021

Direito Digital: Debates Contemporâneos / Coodenação por Ana Paula M. Castro de Lima, Carmina Bezerra Hissa, Paloma Mendes Saldanha – 11Ed- São Paulo: Thomson Reuters, Brasil, 2019

PINHEIRO PECK. Patrícia. **#Direito Digital** 6ª Ed.rev,.atual e ampl. –São Paulo: Saraiva 2016

https://bitcoin.stackexchange.com/questions/70336/**what-is-the-difference-between-root-hash-and-block-hash** - Último acesso em 03/03/2021

Curso Udemy: https://www.udemy.com/bitcoin-ethereum-blockchain/ - acessado em 02/09/2020

https://www.treasy.com.br/blog/bitcoins-blockchain-smart-contracts/-acessado em 03/09/2018

https://www.americanbar.org/groups/**business_law**/publications/blt/2017/09/09_ng.html - Último acesso em 14/10/2018

https://it.toolbox.com/blogs/**the-future-is-blockchain-based-smart-contracts-**122017 - Último acesso em 02/02/2021

https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf - Último acesso em 08 /10/2020

https://link.springer.com/chapter/10.1007/978-3-319-39028-4_9 - Último acesso em 18/10/2018

https://anders.com/blockchain/ - Último acesso em 20/09/2018