UNIVERSIDADE DE BRASÍLIA
Faculdade de Direito
Graduação em Direito

BLOCKCHAIN, CONFIANÇA E DIREITO: UM POUCO ALÉM DO ALARDE

Autor: DAVI ANTÔNIO ARAÚJO SILVA

Orientador: ALEXANDRE KEHRIG VERONESE AGUIAR

Monografia apresentada para a conclusão do curso de Direito na Universidade de Brasília – UnB

Brasília – 2019

Araújo, Davi

Blockchain, Confiança e Direito: Um pouco além do alarde

Araújo. – Brasília, 2019.

Monografia (graduação) – Universidade de Brasília, Faculdade de Direito, 2019

Orientador: Alexandre Kehrig Veronese Aguiar.

1. Direito. 2. Tecnologia. 3.Confiança. 4.Segurança Jurídica. 5.DLT (*Distributed Ledger Technologies*), 6. Blockchain

UNIVERSIDADE DE BRASÍLIA

Faculdade de Direito

Curso de Graduação em Direito

Monografia apresentada à Faculdade de Direito – FD, da Universidade de Brasília – UnB, como requisito para a obtenção de grau de Bacharel em Direito.

BLOCKCHAIN, CONFIANÇA E DIREITO: UM POUCO ALÉM DO ALARDE

Davi Antônio Araújo Silva

Aprovado por

_____

Professor Orientador: Alexandre Kehrig Veronese

_____

Professor: Dr. Othon de Azevedo Lopes

_____

Professor: Dr. Rafael Rabelo Nunes

Brasília, 03 de dezembro de 2019.

DEDICATÓRIA

Ao meu Pai.

AGRADECIMENTOS

À família, aos amigos e colegas de trabalho. Aos colegas de curso e aos professores. Aos membros da banca, que tão prontamente aceitaram o convite. Ao orientador, Professor Veronese, pela gentileza, presteza e inspiração. À minha querida esposa Mirlane, que esteve comigo desde o início, pelo carinho, paciência e apoio.

RESUMO

Este trabalho se destina a analisar a relevância das Tecnologias de Registro Distribuído, com ênfase no *Blockchain*, para o Direito, tendo em vista as grandes expectativas sobre essas tecnologias em nível mundial. Para isso, buscou-se uma definição de confiança aplicável ao tema e a correlação entre Direito e Tecnologia. Além de livros e artigos científicos, a pesquisa foi feita também em portais de notícias especializados, dada a atualidade do assunto e, quando cabível, também em itens do ordenamento jurídico brasileiro e internacional. Como resultado, identificou-se a relevância desse novo conjunto de tecnologias em relação ao Direito e algumas de suas limitações quanto a questões de privacidade. Não se trata de um tema fechado e ainda não há consenso sobre como tratar o assunto e suas ramificações. Particularmente com a popularidade crescente das moedas criptográficas, percebe-se uma lacuna de atuação estatal. Assim, é necessário que se mantenha o foco no cerne da questão: confiança.

Palavras-chave: Direito, Tecnologia, DLT, Blockchain, confiança, privacidade

ABSTRACT

Distributed Ledger Technologies (DLTs), especially Bitcoin´s Blockchain, seems to be a worldwide hype. To understand the relevance of such technologies with Law and thus, for a better understanding of the reasons behind the hype, it is necessary to understand the fundamental sociological quest for trust. In order to harden this understanding, a definition for trust must be found and be broad enough to satisfy both Law and Tech. Since this theme is a new one, in addition to books and scientific articles, this research was also conducted in specialized news portals. As a result, we identified where lies the relevance of this new set of technologies in its convergence with Law and some technological limitations regarding privacy issues. The matter is far from being fulfilled. So far, there is no consensus on how to address the issue and its ramifications. Particularly with the growing popularity of crypto currencies, there is a huge regulation gap. Therefore, the ultimate focus is understanding the underlying matter: trust.

Keywords: Law, Technology, Trust, DLT, Blockchain

LISTA DE ILUSTRAÇÕES

Figura 1: Busca pelo termo "blockchain" 5
Figura 2: Cotação BTC / USD. 6
Figura 3: *Hype Cycle for Blockchain Business*, 2018 7
Figura 4: Correspondência entre a regulação legal e a *Lex Informatica* 20
Figura 5: Tipos de Registro Distribuído 26
Figura 6: Crescimento do *blockchain* do Bitcoin. 34
Figura 7: Criptografia Simétrica 49
Figura 8: Criptografia Assimétrica 50
Figura 9: Visualização do processo de assinatura digital usando curvas elípticas 52
Figura 10: Operações sobre uma curva elíptica 53
Figura 11: Árvore de Merkle com 8 folhas. 56
Figura 12: Assinatura digital baseada em criptografia de chaves públicas. 57
Figura 13: Transações assinadas do Bitcoin 57
Figura 14: Certificado Digital X.509: comparação de versões 58
Figura 15: Infraestrutura de Chaves Públicas 59
Figura 16: Transações num Blockchain 60
Figura 17: Cabeçalho de um bloco 61

LISTA DE TABELAS

Tabela 1: Hash da palavra “unb” por diferentes algoritmos..... 54
Tabela 2:Hash de "Universidade de Brasília" por diferentes algoritmos 54

LISTA DE ABREVIATURAS E SIGLAS

DAO	*Decentralized Autonomous Organization* - Organização Autônoma Descentralizada.
DLT	*Distributed Ledger Technologies* – Tecnologias de Registro (ou de Livro Razão) Distribuído. Neste trabalho, frequentemente será usado como sinônimo "blockchain".
GDPR	*General Data Protection Regulation*. Sinônimo de RGPD.
IoT	*Internet of Things*, Internet das coisas: a interconexão de dispositivos domésticos à internet.
LGPD	Lei Geral de Proteção de Dados, corresponde à Lei nº 13.709/2018.
P2P	*Peer-to-Peer*. Tipo de rede em que os participantes normalmente não têm hierarquia entre si: são pares.
RGPD	Regulamento Geral de Proteção de Dados. Trata-se da lei europeia que dispõe sobre a proteção de dados pessoais e sensíveis.
SCADA	*Supervisory Control and Data Acquisition*: Controle de supervisão e aquisição de dados.
TIC	Tecnologia da Informação e Comunicações.
WEF	*World Economic Forum* – Fórum Econômico Mundial.

SUMÁRIO

INTRODUÇÃO 1
ESTRUTURA DO TRABALHO 2
1. REFERENCIAL TEÓRICO-METODOLÓGICO 4
1.1. Propósito 4
1.2. Metodologia 4
1.3. Resultados 4
1.4. Implicações práticas 4
1.5. Originalidade e relevância 4
2. BLOCKCHAINS – GRANDES ESPERANÇAS 5
3. CONFIANÇA E O DIREITO 9
4. PRINCÍPIOS DA SEGURANÇA JURÍDICA E PROTEÇÃO DA CONFIANÇA NO DIREITO 13
5. VALIDADE DA NORMA NO CIBERESPAÇO 17
6. NADA NOVO DEBAIXO DO CÉU: TECNOLOGIAS DE REGISTRO DISTRIBUÍDO22
7. BLOCKCHAIN E O DIREITO 27
8. PROTEÇÃO DA PRIVACIDADE: LIMITAÇÕES DE DLTs ANTE REGULAÇÃO PARA PROTEÇÃO DE DADOS 31
8.1. MINIMIZAÇÃO DE DADOS 33
8.2. O DIREITO DE RETIFICAÇÃO 35
8.3. O DIREITO DE ACESSO 37
8.4. O DIREITO AO ESQUECIMENTO 39
9. CONCLUSÃO 43
ANEXO A – CRIPTOGRAFIA 48
ANEXO B – FUNÇÕES HASH 54
ANEXO D – ASSINATURA DIGITAL 57
ANEXO E – INFRAESTRUTURA DE CHAVES PÚBLICAS 58
ANEXO F – BITCOIN E BLOCKCHAIN 60

INTRODUÇÃO

A apresentação do programa de "Direito e tecnologia" da Universidade de Harvard[1] ressalta que o Direito se esforça para acompanhar a constante mudança da tecnologia, e que o *estudo de como a lei interage com a ciência e a tecnologia é mais crítico agora do que nunca*.

De fato, relações de consumo, identidade, privacidade, interações sociais, propaganda, propriedade, governo e regulação dependem cada vez mais das tecnologias da informação e comunicações. Dentre essas tecnologias, "Blockchain" tem tido um lugar de destaque como a precursora de uma nova revolução, com diversos "evangelistas" que apregoam suas benesses. Tamanha repercussão dificilmente ocorreria se não houvesse, de fato, algum tipo de utilidade. Ao lidar com assuntos sensíveis, certamente há consequências no âmbito do Direito.

Intuitivamente, com o conhecimento básico do que é *blockchain* e DLTs (*Distributed Ledger Technologies*), percebe-se que sua utilidade reside no estabelecimento de mecanismos de confiança, das garantias necessárias para a relação dos indivíduos entre si e entre instituições, além da necessidade de transparência e previsibilidade.

A confiança não é um tema fechado na filosofia ou na antropologia. Contudo, a sociologia traz definições suficientemente sólidas para começar a compreender o papel da confiança em relação ao Direito. É importante perceber que as leis carecem de validação para serem efetivas, que sua mera existência não é garantia de efetividade ou justiça.

Além disso, as leis são limitadas às suas jurisdições, o que não necessariamente ocorre com as tecnologias da informação e comunicação. Em tempos de internet, a autoridade dos Estados e a efetividade dos poderes instituídos ganham contornos diferentes. Compreender essas novas limitações é fundamental, pois nesse entendimento reside o grande diferencial das tecnologias de registro distribuído, particularmente, *blockchains*.

Porém, seu uso exige cuidado, particularmente no que tange a questões de privacidade.

[1] HARVARD UNIVERSITY, **Law, Science, and Technology** , disponível em < https://bit.ly/2ra6J2a>, acesso em 05/12/2019.

ESTRUTURA DO TRABALHO

O presente trabalho foi dividido em nove capítulos, deixando algumas explicações de caráter mais técnico nos Anexos, pois são importantes para a compreensão do assunto, mas não são pertinentes ao Direito.

O ponto central é tentar responder a seguinte pergunta: por que o assunto "Blockchain" teria relevância para o Direito? Alguns fragmentos para denotar o entusiasmo alardeado sobre o tema, em diversos meios, estão no capítulo "BLOCKCHAINS – GRANDES ESPERANÇAS".

Na busca por resposta, o caminho natural parece ser considerar a natureza do próprio Direito nas relações sociais e a busca por segurança nas relações em geral, seja entre pessoas, seja entre instituições, que convergem para o tema "confiança": o cumprimento de uma expectativa, a esperança de que alguém cumpra uma promessa, uma capacidade de acreditar que alguma coisa funciona sem que se saiba exatamente como.

Nessa trilha, o trabalho do sociólogo Anthony Giddens oferece uma construção bastante segura e de aplicação ampla do que é a confiança em termos sociológicos e sua serventia no entendimento da história, conforme o capítulo "CONFIANÇA E O DIREITO".

Uma vez definida a questão da confiança, compreender um pouco mais a fundo sua relação com o Direito é o próximo passo: no capítulo "PRINCÍPIOS DA SEGURANÇA JURÍDICA E PROTEÇÃO DA CONFIANÇA NO DIREITO", são analisados diversos pensadores que se ocuparam em tentar definir a norma como um instrumento de construção da confiança, de previsibilidade, tanto nos termos gerais observados nos Princípios de Direito quanto em normas suficientemente abstratas para representá-los e algumas de cunho bastante prático, como as Súmulas Vinculantes[2].

A partir da consideração das normas como instrumentos de confiança, é necessário analisar a natureza do relacionamento entre norma e tecnologia. Há discussões bastante antigas acerca de soberania, equilíbrio do poder, privacidade e propriedade, que tomam novos contornos em tempos de internet e que levantam questões como: uma vez que a sociedade cria cada vez mais dependência dos meios de comunicação digital, como manter a confiança? Como

[2] MASSON, N., **Manual de Direito Constitucional**, 7ª ed., Editora Jus Podivm, p. 905: "Súmulas são enunciados que explicitam, de maneira concisa, a interpretação de um Tribunal a respeito de determinados temas. Têm por intuito descongestionar os trabalhos do Tribunal, por meio da fixação do entendimento acerca de assuntos que corriqueiramente se apresentam, e uniformizar as respostas estatais ofertadas aos jurisdicionados, fazendo valer o brocardo da isonomia que preceitua que casos semelhantes devam ser destinatários de soluções semelhantes."

os paradigmas legais aplicam-se ao ciberespaço[3]? No Capítulo "VALIDADE DA NORMA NO CIBERESPAÇO", discute-se o trabalho de pensadores como Joel Reidenberg e Lawrence Lessig, que criaram teorias para tratar o assunto, considerando primeiro um paralelismo entre as normas e suas limitações no "mundo real" em relação a essas normas no "mundo digital".

No Capítulo "NADA NOVO DEBAIXO DO CÉU: TECNOLOGIAS DE REGISTRO DISTRIBUÍDO", discute-se o aparecimento da rede Bitcoin[4] em 2008, que oferece um meio de troca e acumulação totalmente descentralizado e, *a priori*, dependente apenas dos seus membros. Essa rede oferece mecanismos de transparência para cada transação e privacidade vinculada a esquemas engenhosos de uso de criptografia[5]. Com essa rede, ganhou atenção também o mecanismo que permite seu funcionamento: o *blockchain*, uma implementação peculiar de DLT[6] aberta, passível de uso em diversos tipos de situação em que singularidade e transparência de registros são características importantes.

Dadas as novas discussões sobre proteção da privacidade e o *hype*[7] criado em torno dessas tecnologias de registro, há questões bastante sensíveis ainda não resolvidas, que autores como Michèle Finck[8], Primavera De Filippi[9] e Kevin Werbach[10] buscam analisar com profundidade e sob diferentes pontos de vista, conforme o capítulo "BLOCKCHAIN E O DIREITO".

Finalmente, o capítulo "PROTEÇÃO DA PRIVACIDADE: LIMITAÇÕES DE DLTs ANTE REGULAÇÃO PARA PROTEÇÃO DE DADOS" discute algumas limitações técnicas impostas por essas tecnologias, conforme observado por Michèle Finck.

---

[3] "Ciberespaço" tem sua origem na "cibernética", termo usado por Norbert Wiener na década de 1940 para tratar a interface entre seres vivos e máquinas de maneira interdisciplinar, tendo repercussões tanto nas artes quanto nas ciências (MÜLLER, A., **A Brief History of the BCL**, 2000, disponível em <https://bit.ly/2MXzLdb> acesso em 11/09/2019). O termo "Ciberespaço" aparece a primeira vez na década de 1960 na obra de Susanne Ussing e se popularizou na década de 1980 com os trabalhos ficção científica de William Gibson. Posteriormente, de 1990 em diante, é frequentemente usado como sinônimo de internet, embora não o seja (LESSIG, L, **CODE 2.0**, 1999).

[4] Vide Anexo F.

[5] Vide Anexo A.

[6] Vide capítulo "6. NADA NOVO DEBAIXO DO CÉU: TECNOLOGIAS DE REGISTRO DISTRIBUÍDO"

[7] "Hype" é uma palavra utilizada para qualificar que há o exagero de algo, ou em marketing uma estratégia para enfatizar alguma coisa, ideia ou um produto. Mais informações, vide <https://bit.ly/2JzUNws>, acesso em 31/10/2019.

[8] Michèle Finck é pesquisadora sênior do Instituto Max Planck de Inovação e Competição, em Munique, pesquisadora na University College London e como acadêmica no Centro de Regulação da Europa ('CERRE') sobre integração entre direito, tecnologia, inovação e direitos fundamentais. Mais informações em <https://michelefinck.eu>. Acesso em 20/10/2019.

[9] Primavera De Filippi é pesquisadora da CERSA (Universidade Paris II) e pesquisadora associada da Universidade de Harvard. Estuda implicações legais das arquiteturas distribuídas, com foco em tecnologias blockchain. Mais informações em <http://cersa.cnrs.fr/de-filippi-primavera/>. Acesso em 30/10/2019.

[10] Kevin Werbach é advogado e professor da Wharton School (University of Pennsylvania) especialista em implicações comerciais, legais e sociais de tecnologias emergentes, como blockchain, banda larga e *big data.* Mais informações em <http://werbach.com/ >. Acesso em 30/10/2019.

1. REFERENCIAL TEÓRICO-METODOLÓGICO

1.1. Propósito

Este trabalho visa analisar a relevância para o Direito das DLTs, particularmente os baseados no *blockchain* do *Bitcoin*, tendo em vista o alarde midiático sobre o assunto nos últimos anos, considerando, em especial, a proteção de dados pessoais.

1.2. Metodologia

Foi feita pesquisa bibliográfica em textos de autores do Direito, Sociologia e artigos científicos, tratando diferentes pontos de vista de direito e tecnologia. Como fonte de dados estatísticos, foi utilizada pesquisas da ferramenta *Trends*™ do Google™. Como motivadores, alguns textos da mídia especializada. A maior parte da literatura consultada provém de fontes estrangeiras, que foram traduzidas livremente.

1.3. Resultados

Foram identificadas definições sobre os temas e suas correlações, tendo como ponto central o *blockchain*, no intuito de aferir bases mais sólidas de sua relevância para o Direito.

1.4. Implicações práticas

Tal como ocorre com novas tecnologias, existe alarde sobre suas potencialidades, que criam grandes expectativas. Com o gradativo amadurecimento dessas expectativas, há um descrédito natural, que perdura até que se encontre um novo patamar de maturidade, que se desenvolva uma nova confiança e, neste momento, é possível falar de seu uso prático. Na atualidade, a preservação da privacidade tem sido discutida com muita frequência. No caso brasileiro, a questão tem especial relevância em razão da Lei Geral de Proteção de Dados.

1.5. Originalidade e relevância

Neste estudo, busca-se construir uma base sociológica para a construção da confiança e a utilidade do Direito, que se utilizam dos recursos disponíveis em seu tempo e espaço para manter a ordem e criar prosperidade, sempre considerando questões como a preservação da confiança em geral e o relacionamento entre os diferentes atores.

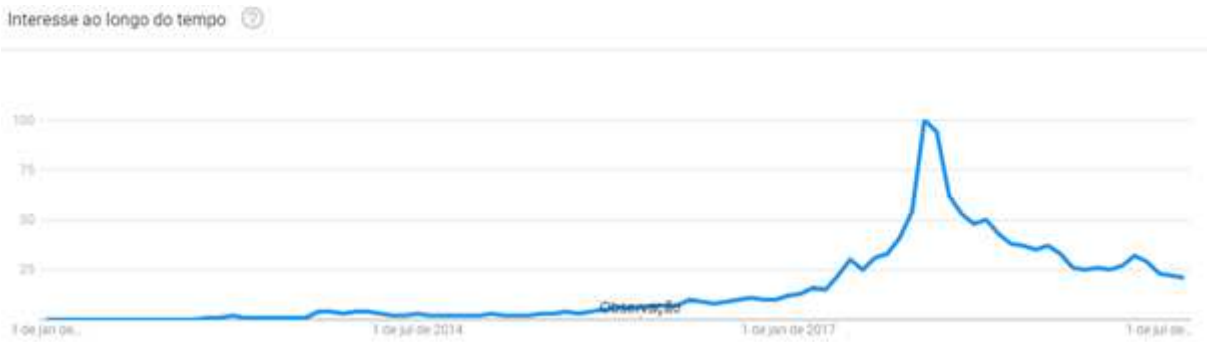
2. BLOCKCHAINS – GRANDES ESPERANÇAS

CASTELLS(1999)[11] considera que o destino de uma sociedade depende fortemente de sua habilidade ou falta de habilidade em dominar tecnologias, especialmente as mais estratégicas, mais relevantes num determinado período histórico. Embora não se possa afirmar que a tecnologia (ou a falta dela) por si só determine uma mudança social, é possível afirmar que ela reflete a capacidade das sociedades de se transformarem, de se adaptarem, e que as transformações que não ocorrem de maneira igual em todos os lugares.

Novas tecnologias são maleáveis e podem se desenvolver em diversas direções: é neste ponto que Negócios, Tecnologia e o Direito devem se encontrar, a fim de que o diálogo entre técnicos e reguladores ocorra para garantir a inovação em prol do bem público (FINCK, 2018)[12].

Dentre as inovações atuais, as Tecnologias de Registro Distribuído (*Distributed Ledger Technologies* – DLTs) têm criado grandes expectativas, com particular destaque para a tecnologia por trás do Bitcoin: *blockchain.* Pela Figura 1, que mostra que a frequência de busca por termos no Google, percebe-se que o interesse por "blockchain" é bastante recente:

Figura 1: Busca pelo termo "blockchain"

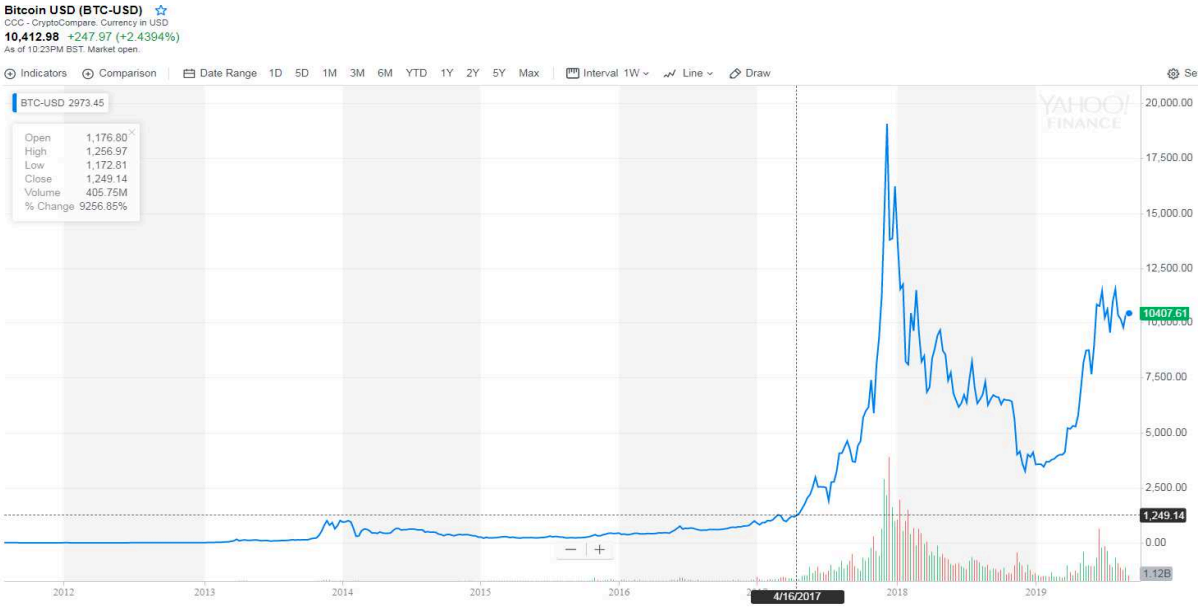


Fonte: ferramenta <https://trends.google.com>. Consulta em 12/09/2019

Percebe-se que o aumento do interesse é quase abrupto e coincide com a grande valorização do Bitcoin que ocorreu há quase dois anos mostrado na Figura 2:

[11]CASTELLS, M. 1999. **La Era de la información: economía, sociedad y cultura**. México: Siglo Veintiuno Editores, 1999, p. 32, disponível em <https://bit.ly/30dApHQ>, acesso em 20/09/2019.
[12] FINCK, M., **Blockchains and Data Protection in the EU**, 2018, disponível em <https://bit.ly/2NE4NaA>, acesso em 11/09/2019, p. 21.

Figura 2: Cotação BTC / USD.



Fonte: Yahoo Finance, disponível em: <https://yhoo.it/2kjdafQ>. Acesso em 12/09/2019.

Há grande otimismo no mundo em relação ao uso dessas tecnologias. O portal The Economist[13] fala da "grande corrente para ter certeza das coisas"; o Yahoo Finance[14] menciona que "o Blockchain é uma das tecnologias mais revolucionárias desta geração e tem aplicativos que se espalham por todos os setores da nossa economia"; o Deutsche Welle[15], que "Especialistas veem o potencial de uma revolução digital que poderia um dia tornar os bancos obsoletos"; já o banco Goldman Sachs[16] afirma que o "*Blockchain* tem o potencial de mudar a forma com que vendemos e compramos, interagimos com o governo, verificamos a autenticidade de tudo, desde imóveis até produtos orgânicos". De acordo com o IDC Group[17], espera-se um investimento global de aproximadamente U$2.9 bilhões em 2019. NOTHEISEN *et al* (2017, pg. 1062)[18] explica que

---

[13] THE ECONOMIST, **Blockchains: The great chain of being sure about things**, 31/10/2015, disponível em <https://econ.st/2IFp6Ds>, acesso em 23/09/2019.

[14] YAHOO FINANCE, **Blockchain Is Revolutionizing The Way We Do Business**, 20/08/2019, disponível em <https://yhoo.it/2l7I3nN>, consultado em 21/09/2019.

[15]DEUTSCHE WELLE, **Blockchain: Paying with bits and bytes**, 10/05/2019, disponível em <https://bit.ly/2mdu2VQ>, consultado em 23/09/2019.

[16] GOLDMAN SACHS, **Blockchain - The new technology of trust**, disponível em <https://bit.ly/2Lpctck>, consultado em 23/09/2019.

[17] IDC GROUP, **Worldwide Blockchain Spending Forecast to Reach $2.9 Billion in 2019, According to New IDC Spending Guide**, 04/03/2019, disponível em <https://bit.ly/2F5c8vy>, consultado em 23/09/2019.

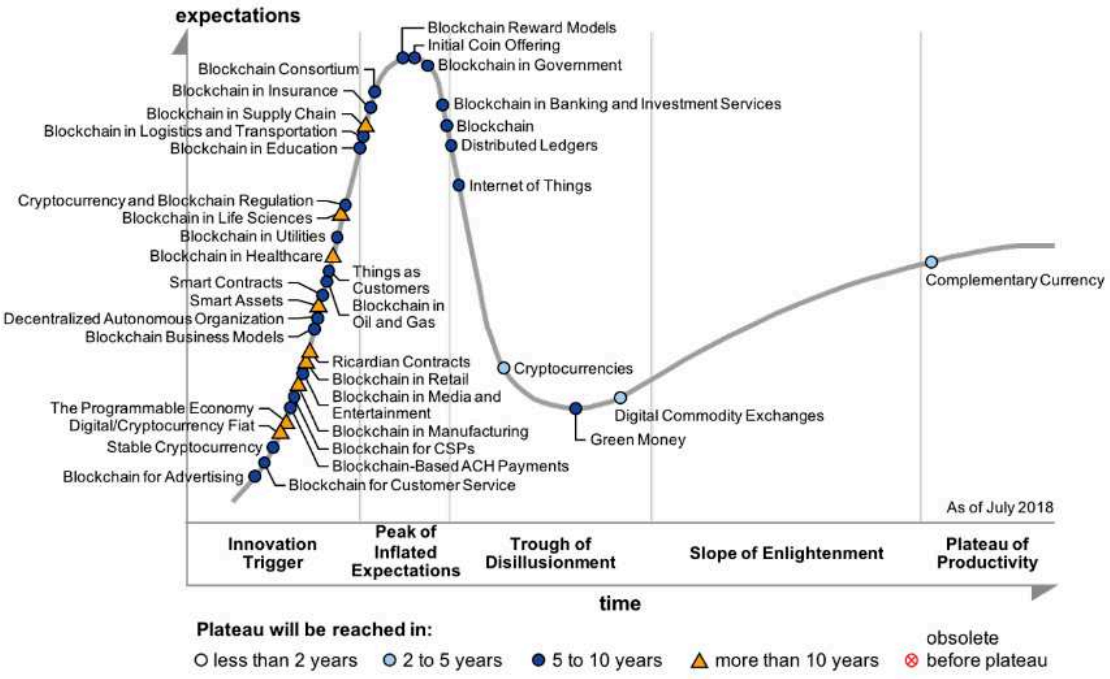
[18] NOTHEISEN, B.; HAWLITSCHEK, F, WHINHARDT, C., **Breaking down the Blockchain hype - towards a Blockchain market engineering aproach**. *In* Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017, "In fact, the blockchain is frequently referred to as one of

> De fato, o *blockchain* é frequentemente referido como uma das principais inovações tecnológicas do século XXI que tem o potencial de remodelar e interromper uma infinidade de atividades econômicas, como transações consumidor-consumidor no domínio da economia compartilhada ou bancária.

Como contraponto, o Fórum Econômico Mundial[19] (*World Economic Forum* - WEF) faz a seguinte ponderação: "(O *blockchain*) Foi proposto como uma solução para uma variedade tão estonteante de problemas e indústrias que é cada vez mais difícil acompanhar, e muito menos desenvolver uma abordagem racional e sensata da tecnologia."

Em 2018, o Grupo Gartner publicou seu *hype cycle* sobre aplicações para negócios:

Figura 3: *Hype Cycle for Blockchain Business*, 2018



Fonte: Gartner, disponível em <https://gtnr.it/2LsRSY2>. Acesso em 01/09/2019

O fato de que a maior parte das aplicações consideradas na Figura 3 encontrarem-se em fase de inovação ou expectativas infladas denota que ainda há muito o que se amadurecer: existe

---

the main technological innovations of the 21st century that has the potential to reshape and disrupt a plethora of economic activities such as consumer to consumer transactions in the realm of the sharing economy or banking".

[19]WEF, **Blockchain Beyond the Hype A Practical Framework for Business Leaders**, 2018, tradução livre, disponível em <https://bit.ly/2HoLWL2>, acessado em 11/09/2019.

grande potencial a ser explorado nos mais diversos campos, mas há diversos problemas com sua adoção a serem resolvidos.

Em 2015, WEF[20] divulgou dados oriundos de entrevistas em que a maior parte dos entrevistados esperava que 10% do PIB mundial estivesse armazenado com base em alguma implementação de *blockchain*. Em 2018, devido ao excessivo entusiasmo despertado pelo assunto, o WEF[21]publicou um novo documento instruindo que:

> Um dos aspectos mais relevantes do *blockchain* é seu alto número de evangelistas - pessoas que acreditam que o *blockchain* pode resolver tudo, desde a desigualdade financeira global ao acesso ao financiamento para *start-ups*, fornecimento de identificação para refugiados, resolução de problemas da cadeia de suprimentos e capacitação de pessoas para vender suas casas sem precisar de um agente imobiliário. Começou a parecer que os mais intratáveis problemas do mundo estavam apenas esperando a chegada do *blockchain*. Isso não é apenas enganoso, mas também se torna uma barreira para os tomadores de decisão em uma perspectiva equilibrada da tecnologia.

"Blockchain" é um tipo de tecnologia de registro distribuído proposto no artigo que deu origem ao Bitcoin. É necessário ressaltar que todo *blockchain* é uma tecnologia de registro distribuído, mas nem todo registro distribuído é um *blockchain*, embora seja comum que a literatura atual trate como sinônimos.

Nas palavras de DE FILIPPI *et al* (2015)[22]:

> Estamos à beira de uma nova revolução digital. A Internet está iniciando uma nova fase de descentralização. Após mais de vinte anos de pesquisa científica, houve avanços dramáticos nos campos de criptografia e redes de computadores descentralizadas, resultando no surgimento de uma nova tecnologia profunda - conhecida como *blockchain* - que tem o potencial de mudar fundamentalmente a maneira como a sociedade opera.

---

[20] WEF, "**Deep Shift Technology Tipping Points and Societal Impact, Survey Report**", 2015, disponível para consulta pública pela internet em <https://bit.ly/1KlN8ZR>. Acesso em 05/09/2019.

[21] *Idem*, "**Blockchain Beyond the Hype A Practical Framework for Business Leaders**", 2018, "One of the most unique aspects of blockchain is its high number of evangelists – people who believe blockchain can solve everything from global financial inequality to access to financing for start-ups, the provision of ID for refugees, to solving supply chain problems and enabling people to sell their houses without needing an estate agent. It has started to seem that the most intractable of the world's problems have merely been waiting for blockchain to arrive. This is not only misleading and untrue but also becomes a barrier to decision-makers in taking a balanced perspective on the technology".

[22] DE FILIPPI, P., WRIGHT, A., **Decentralized Blockchain Technology and the Rise of Lex Cryptographia**, 2015, disponível em <https://bit.ly/1JXbOxe>, acesso em 14/10/2019. "We stand at the edge of a new digital revolution. The Internet is beginning a new phase of decentralization. After over twenty years of scientific research, there have been dramatic advances in the fields of cryptography and decentralized computer networks, resulting in the emergence of a profound new technology—known as the blockchain— which has the potential to fundamentally shift the way in which society operates. The blockchain is a distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information. It enables, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority".

> O *blockchain* é um banco de dados distribuído, compartilhado e criptografado que serve como um repositório público de informações irreversíveis e incorruptíveis. Permite, pela primeira vez, que pessoas não relacionadas cheguem a um consenso sobre a ocorrência de uma transação ou evento específico sem a necessidade de uma autoridade de controle.

Por trás de todas as propagandas dos mais diferentes usos, por trás do discurso dos entusiastas e do trabalho feito por desenvolvedores ao redor do mundo, há uma busca muito mais antiga: uma busca por garantias, por transparência, controle e agilidade. Diante do exposto, depreende-se que há uma busca pela garantia de segurança e confiança, tanto de maneira concreta, por meio da construção de mecanismos e instrumentos que as assegurem, quanto de forma abstrata, pelas constantes mudanças de entendimento advindas da discussão de seus limites e significados nos mais diversos contextos.

3. CONFIANÇA E O DIREITO

Viver em sociedade é aderir a diversos valores e comportamentos que tornam a convivência possível. Em sociedades primitivas, indivíduos nascem e crescem com determinados costumes e com laços naturais que determinam, ainda de maneira rudimentar, a moral e a autoridade, vinculados ao parentesco, amizade e, mais tarde, relações clientelistas[23]. Limites de tempo e espaço são mais próximos, sem necessidade de estado organizado, leis escritas ou a delegação de autoridade. A mera convivência é a fonte da confiança entre os indivíduos.

Com o crescimento demográfico e desenvolvimento social, indivíduos vivendo no mesmo tempo e no mesmo espaço geográfico passam a precisar de acordos[24] entre si para que possam conviver. Nasce a necessidade de estruturas e funções em que os indivíduos de alguma maneira *reconhecem* ou *delegam* poder e atribuições a terceiros. Tanto esse reconhecimento quanto a delegação envolvem "Confiança", que significa basicamente fé[25], crédito, crença ou

---

[23]BANTON, M., **The Social Anthropology Of Complex Societies.** New York: Frederick A. Praeger, 1966, p. 1-18.

[24] Na filosofia moral e política, o "acordo" ou "contrato social" são teorias que se popularizaram durante o Iluminismo para tentar compreender a construção da legitimidade da autoridade do estado sobre o indivíduo.

[25]GIDDENS, A., **As Consequências da Modernidade**. São Paulo: Editora Unesp, 1991, disponível em <https://bit.ly/1CQiUQb>, consulta em 07/09/2019, p. 25: " A confiança, em suma, é uma forma de "fé" na qual a segurança adquirida em resultados prováveis expressa mais um compromisso com algo do que apenas uma compreensão cognitiva."

expectativa: trata-se da forma de encontrar algum tipo de previsibilidade, assumindo a existência de incertezas, de riscos.

No que se pode chamar de "Modernidade"[26], a noção de tempo e espaço se altera: GIDDENS(1990) nos ensina que a concepção de tempo e espaço é diferente em sociedades tradicionais e sociedades modernas: nas pré-modernas, as conexões são físicas, o que significa dizer que tempo e espaço estão juntos quando pessoas se juntam[27]; nas modernas[28], tempo e espaço não necessariamente são coincidentes. Há um desencaixe (*disembedding*), um "deslocamento" das relações sociais para extensões indefinidas, atemporais, viabilizado pela construção da confiança nas instituições e em seus delegados. BOURDIEU(2014)[29] confirma esse pensamento ao afirmar que instituições:

> São o fiduciário organizado, a confiança organizada, a crença organizada, a ficção coletiva reconhecida como real pela crença e, por isso, tornando-se real. Evidentemente, dizer de uma realidade que ela é uma ficção coletiva é uma maneira de dizer que isso existe fantasticamente, mas não como acreditamos que exista.

Os avanços tecnológicos e as instituições em geral, a que Antony Giddens chama de sistemas peritos (*expert systems*), representam a confiança depositada no conhecimento e habilidade de terceiros, que permitem que se utilize determinada benesse sem que haja qualquer tipo de conhecimento do mecanismo ou nos detalhes de sua construção. Carros, aviões, edifícios, máquinas em geral, sistemas burocráticos, governos e a própria internet são exemplos de sistemas peritos.

Esses sistemas podem necessitar de símbolos físicos e abstratos para garantirem privilégios ou características especiais aos seus portadores, com grande aceitação nos limites de alguma comunidade, como o dinheiro, como a legitimidade política de um governante,

---

[26] *Idem, Ibdem*, p. 6: "Modernidade" refere-se ao estilo, costume de vida ou organização social que emergiram na Europa a partir do século XVII e que ulteriormente se tornaram mais ou menos mundiais em sua influência. Isto associa a modernidade a um período de tempo e a uma localização geográfica inicial, mas por enquanto deixa suas características principais guardadas em segurança numa caixa preta".

[27] *Idem, Ibdem*, p. 22: "Nas sociedades pré-modernas, espaço e tempo coincidem amplamente, na medida em que as dimensões espaciais da vida social são, para a maioria da população, e para quase todos os efeitos, dominadas pela "presença" - por atividades localizadas".

[28] *Idem, Ibdem*, p. 23-24 "A separação entre tempo e espaço e sua formação em dimensões padronizadas, "vazias", penetram as conexões entre a atividade social e seus "encaixes" nas particularidades dos contextos de presença. As instituições desencaixadas dilatam amplamente o escopo do distanciamento tempo-espaço e, para ter este efeito, dependem da coordenação através do tempo e do espaço. Este fenômeno serve para abrir múltiplas possibilidades de mudança liberando das restrições dos hábitos e das práticas locais."

[29] BOURDIEU, P, **Sobre o Estado: Cursos no Collège de France (1989-92)**, Ed. Companhia das Letras, 2014, p. 91.

documentos de identidade, patentes militares, certificados digitais. São os emblemas ou fichas simbólicas (*symbolic tokens*).

Esses sistemas e símbolos são o fruto da consciência geral que a atividade humana não ocorre por influência divina ou natureza, mas socialmente. A ação humana cria instituições que simultaneamente aumentam sua coesão e seu espaço, seu conforto e abundância. O acaso e o perigo não deixam de existir, mas eles tomam a forma de risco, que é a consciência de que resultados adversos possam ocorrer. Nascem as ideias de "risco calculado" (em que destreza e acaso são fatores considerados), "risco aceitável" (advindo da minimização do perigo), "ambientes de risco" (que afetam coletividades) e "segurança" (situação em que perigos são neutralizados).[30]

É possível afirmar, portanto, que "confiar" é um fenômeno que ocorre na falta de informação plena, não na falta de poder. A confiança ocorre quando não há visibilidade e a contingência encontra base na suposição de credibilidade, numa expectativa de resultado e comportamento, na crença de uma determinada pessoa ou sistema, expressa como fé na probidade ou na correção de princípios abstratos. Com efeito, GIDDENS(1991) afirma que toda confiança é, num certo sentido, cega.

Com o intuito de aumentar a previsibilidade das relações, fazendo com que seus riscos intrínsecos fossem mais aceitáveis, os costumes tiveram de evoluir para as leis em algum momento da história das sociedades modernas. LÉVY-BRUHL(1997)[31] chama a atenção que a lei é posterior ao costume por necessitar de linguagem escrita e lembra que, na antiguidade, não havia diferença entre o sistema legal e religião: são as questões de tempo-espaço que coincidem, que criam familiaridade entre os membros. A lei escrita é um tipo de emblema simbólico, cuja validade aumenta significativamente seu espaço e permanece no tempo para muito além de seus promulgadores. Embora com ressalvas, é possível dizer que a lei é um emblema que atende às características elementares da confiança propostas por LUHMANN(2009)[32]:

> A confiança supõe três características elementares:
> (a) permanência dos estados, de modo que se igualem presente e futuro;
> (b) simplificação por meio da redução da complexidade e das infinitas possibilidades variáveis;
> (c) antecipação do futuro, pela projeção daquilo que se dá no presente, para tempos vindouros.

---

[30] GIDDENS, A., **As Consequências da Modernidade**. São Paulo: Editora Unesp, 1991, disponível em <https://bit.ly/1CQiUQb>, consulta em 07/09/2019, p. 35 a 37.
[31] LÉVY-BRUHL, H., **Sociologia do Direito**, Ed. Martins Pena, 1997, pg. 56.
[32] LUHMANN, N., **Introdução à teoria dos sistemas.** 3ª. ed. Petrópolis: Vozes, 2009, p. 328.

BANAKAR(2015)[33] afirma que a lei é um dos poucos instrumentos que se pode empregar para aumentar o grau de certeza nas questões sociais: o cerne do Estado de Direito está na promessa de certeza e uniformidade em questões legais e a incerteza, neste contexto, só tem conotações negativas. Isso significa dizer que a segurança no Direito é um dos pilares do Estado[34]. Neste ponto, percebe-se um ciclo: o Direito se sustenta na confiança e, para isso, cria em si mecanismos para protegê-la.

No caso específico do Brasil atual, DI PIETRO(2019)[35] lista diversos normativos para tratar especificamente a confiança sistêmica, a começar pelo inciso XXXVI[36] do Art. 5º da Constituição Federal de 1988 (CF/88), que tem atrelado a si as Súmulas Vinculantes 1[37], 9[38] e 35[39]. O próprio uso de súmulas vinculantes, conforme preconizado no §1º do Art. 103-A da CF/88, é uma questão de segurança e confiança[40], que reverbera em todo o ordenamento

---

[33] BANAKAR, R., **Normativity in Legal Sociology**, Ed. Springer, 2015, p. 13 e 14: "Law is amongst the few formal tools we can employ to enhance certitude in human affairs. Central to "the rule of law" (*Rechtssicherheit*) is the promise of certainty and uniformity in legal decision-making. Understandably, the focus of legal theory as well as socio-legal research has been traditionally on certainty, i.e. on the mechanisms which help to ensure law's internal operations and safeguard expectations and expectation of expectations in social relations and institutional activities. Attempts to close the gap between "law in books" and "law in action," which we discussed above, also belong to the search for legal certainty. Efforts to harmonise various categories of legal rules (commercial law is the best example) across national boundaries are also motivated by the belief that by increasing similarities between legal systems we enhance certitude, thus improving law's efficiency. Uncertainty, on the other hand, has only negative connotations. At best, it draws attention to areas of social life which are in need of control—where law should be brought in to create certainty by securing expectations—and at worst, it highlights the failures of the law. Talking about emerging uncertainties amounts to challenging orthodoxies and beliefs in the force of rationality, universal values and norms which continue to inform traditional social and legal theories."

[34] KNIJNIK, D., **O princípio da segurança jurídica no direito administrativo e constitucional**. Revista do TCE-RS, v. 13, p. 148: "(...) a segurança jurídica é antes de tudo, um valor subjacente a toda e qualquer compreensão de direito".

CASTILLO BLANCO, F. A. **La protección de confianza en el derecho administrativo**, p. 63: "(...) sin siguridad jurídica, podríamos decir para acabar la idea, puede resultar una quimera hablar con propriedad de Estado de Derecho."

[35] DI PIETRO, M. S. Z., **O STJ e o princípio da segurança jurídica**, Portal Migalhas, 14/05/2019, disponível em <https://bit.ly/335cR9x>, acesso em 31/10/2019.

[36] BRASIL, **Constituição da República Federativa do Brasil,** de 5 de outubro de 1988, Art. 5º, "XXXVI - a lei não prejudicará o direito adquirido, o ato jurídico perfeito e a coisa julgada".

[37] _____, Supremo Tribunal Federal, **Súmula Vinculante 1**: "Ofende a garantia constitucional do ato jurídico perfeito a decisão que, sem ponderar as circunstâncias do caso concreto, desconsidera a validez e a eficácia de acordo constante de termo de adesão instituído pela LC 110/2001", 2007.

[38] _____, **Súmula Vinculante 9**: "O disposto no art. 127 da Lei 7.210/1984 (LEP) foi recebido pela ordem constitucional vigente, e não se lhe aplica o limite temporal previsto no caput do art. 58.", 2008.

[39] _____, **Súmula Vinculante 35**: "A homologação da transação penal prevista no art. 76 da Lei 9.099/1995 não faz coisa julgada material e, descumpridas suas cláusulas, retoma-se a situação anterior, possibilitando-se ao Ministério Público a continuidade da persecução penal mediante oferecimento de denúncia ou requisição de inquérito policial.", 2014.

[40] _____, **Rcl 10.707 AgR, voto do rel. min. Celso de Mello**: "(*A súmula vinculante*) há de ser entendida, em face das múltiplas funções que lhe são inerentes – função de estabilidade do sistema, função de segurança jurídica, função de orientação jurisprudencial, função de simplificação da atividade processual e função de previsibilidade decisória (...)", 2014, disponível em <https://bit.ly/2kqGxga>, acesso em 11/09/2019.

jurídico. O Código de Processo Civil (CPC/15, Lei Nº 13.105/2015), nos Artigos 927, 975, 985 e 987, trata explicitamente da aplicação sumular em decisões sempre quando forem cabíveis. A Lei de introdução às normas do Direito Brasileiro (Decreto-Lei 4.657/1942, LINDB), particularmente em seu Art. 24[41], demanda o respeito às decisões.

Em nível mais abstrato, busca-se a proteção da segurança jurídica e da confiança.

4. PRINCÍPIOS DA SEGURANÇA JURÍDICA E PROTEÇÃO DA CONFIANÇA NO DIREITO

DI PIETRO(2019)[42], FERREIRA(2015)[43] e ÁVILA(2012)[44] colocam o princípio da proteção à confiança e à segurança jurídica como fruto da jurisprudência alemã pós Segunda Guerra Mundial. Colocando um adendo histórico, MAURER(2016)[45] nos conta que o princípio da proteção à confiança tem sua origem num julgado do tribunal administrativo de Berlim de 1957, numa análise entre o princípio da legalidade e a segurança jurídica: pela legalidade, a administração poderia invalidar seus atos com efeitos *ex tunc*; pela segurança , que tem base axiológica na certeza jurídica, boa-fé e lealdade entre as partes. A retratabilidade e invalidação de atos administrativos com benefícios a terceiros passou a ser limitada, em nome da proteção à confiança dos administrados. Em 1976, o Processo Administrativo Alemão consagra de vez este princípio (*Verwaltungsverfahrensgesetz*).

Conceitualmente DI PIETRO(2019) coloca a proteção da confiança como o aspecto subjetivo da segurança jurídica, afirmando, de maneira semelhante ao entendimento da Corte Alemã, que se trata da tutela da proteção da confiança dos indivíduos na licitude de atos

---

[41]BRASIL, LINDB, **Decreto-Lei 4.657/1942**, "Art. 24 A revisão, nas esferas administrativa, controladora ou judicial, quanto à validade de ato, contrato, ajuste, processo ou norma administrativa cuja produção já se houver completado levará em conta as orientações gerais da época, sendo vedado que, com base em mudança posterior de orientação geral, se declarem inválidas situações plenamente constituídas.."
Parágrafo único. Consideram-se orientações gerais as interpretações e especificações contidas em atos públicos de caráter geral ou em jurisprudência judicial ou administrativa majoritária, e ainda as adotadas por prática administrativa reiterada e de amplo conhecimento público.

[42] DI PIETRO, M. S. Z., **O STJ e o princípio da segurança jurídica**, Portal Migalhas, 15/05/2019, disponível em <https://bit.ly/2k5zKII>, acessado em 11/09/2019.

[43] FERREIRA, P. C. A., **O Princípio da Confiança: Proteção e Tópica Jurisprudencial dos Contratos de Saúde Suplementar**, Revista de Direito Civil Contemporâneo, vol. 2/2015, p. 83 – 107, Jan - Mar / 2015, disponível em <https://bit.ly/2kvPhBU>, acesso em 11/09/2019.

[44] AVILA, H., **Segurança jurídica: entre permanência, mudança e realização no direito tributário**. 2. ed. São Paulo: Malheiros, 2012, p. 368-369.

[45] MAURER, H., **Direito Administrativo Geral**, Ed. Manole, 2006.

praticados pela Administração Pública e por terceiros. ÁVILA(2012) faz uma distinção mais detalhada, apresentando diferentes dimensões para tratar a questão (grifos meus):

> O princípio da proteção da confiança (*Vertrauensschutzprincip, principe de protection de la confiance légitime, principle of protection of legitimate expectations*) é diferenciado do princípio da segurança jurídica pelos seguintes critérios: **(a) âmbito normativo** – enquanto o princípio da segurança jurídica diz respeito ao ordenamento jurídico como um todo, focando o âmbito macrojurídico, o princípio da confiança legítima relaciona-se com um aspecto normativo do ordenamento jurídico, enfatizando um âmbito microjurídico; **(b) âmbito pessoal** – enquanto o princípio da segurança jurídica representa uma norma objetiva, não necessariamente vinculada a um sujeito específico, o princípio da confiança legítima protege o interesse de uma pessoa específica; **(c) nível de concretização** – enquanto o princípio da segurança jurídica refere-se, primordialmente, ao plano abstrato, o princípio da confiança legítima pressupõe o nível concreto de aplicação; **(d) amplitude subjetiva de proteção** – enquanto o princípio da segurança jurídica serve de instrumento de proteção de interesses coletivos, o princípio da proteção da segurança jurídica é neutro com relação ao interesse dos cidadãos, podendo tanto ser usado em seu favor quanto em seu desfavor, o princípio da proteção da confiança só é utilizado com a finalidade de proteger os interesses daqueles que se sentem prejudicados pelo exercício passado de liberdade juridicamente orientada.

Nessa linha, no que tange ao Direito, é possível afirmar que proteger a confiança e a segurança jurídica está diretamente relacionado com o próprio valor das normas jurídicas. Nesse intuito, Norberto Bobbio[46] propõe que o valor de uma norma jurídica deva obedecer a três critérios: Justiça, Validade e Eficácia. Em nível epistemológico, cada um desses critérios se relaciona com diferentes problemas: um deontológico, um ontológico e um fenomenológico.

Por problema deontológico do Direito, entenda-se a busca de valores supremos. Nesse entendimento de justiça, trata-se de compreender se a norma reflete esses valores: se há algum tipo de correspondência entre a norma ideal e a real. É um problema resolvido como juízo de valor.

O problema ontológico, que remete a KELSEN (1998)[47], está num "dever ser", em que a norma estaria válida por existir, quer seja posta ou consuetudinariamente. Por esse critério, a validade da norma está condicionada à sua existência, vinculada a um juízo do fato, levando em conta a validade de quem a emanou, se não contradiz uma norma prévia (ab-rogada) acerca da mesma matéria e se encontra harmônica com normas hierarquicamente superiores dentro do mesmo sistema jurídico.

---

[46] BOBBIO, N., **Teoria da Norma Jurídica**, 1ª ed., Bauru, Edipro, 2001, p. 45 a 62.
[47] KELSEN, H., **Teoria pura do Direito**, 6ª ed, Ed. Martins Fontes, São Paulo,1998, p. 158.

O problema fenomenológico diz respeito à aceitação social da norma, da coerção iminente no caso de violação, dado que a simples existência e validade de uma norma não constitui, *a priori*, sua eficácia social.

Embora essenciais a uma norma, essas dimensões são independentes entre si. Isso significa que uma norma podes ser justa, porém inválida e/ou ineficaz; válida, mas injusta e/ou ineficaz; eficaz, porém injusta e/ou inválida. Para exemplificar essa problemática, Bobbio discute normas abstratas, que nunca encontram fulcro que as materialize dentro de um sistema jurídico válido ou, noutros casos, a expectativa abstrata não encontra lugar na prática social. Também se discute aqueles casos em que a norma válida, posta ou costumeira, mas já não representa mais o ideal de justiça de um determinado *zeitgeist* (como leis de segregação racial) ou não encontra reconhecimento prático sobre aqueles que regem (como a lei seca que vigorava nos Estados Unidos entre as duas Guerras Mundiais). É possível perceber também a existência de costumes dentro de um sistema jurídico positivo que nunca são formalizados (eficazes, porém inválidos) ou consensos gerais que outrora foram considerados "direitos naturais" (como a escravidão).

Apesar dessa distinção entre esses elementos, não há precisão entre os critérios de Justiça, Validade e Eficácia das normas. O problema da justiça elucida valores supremos do direito (fins sociais e leis), criando bases para a teoria da justiça. De maneira similar, o problema da validade trata da consistência do direito, "os meios para os fins", de que trata a Filosofia do Direito como Teoria Geral do Direito (BOBBIO, 2001): seu reconhecimento dentro de um sistema normativo deve ocorrem em conjunto com instrumentos de coação que tornem a observação da norma obrigatória, no intuito de criar seus limites e permitir sua modificação dinâmica, tanto no sistema obrigatório quanto a noção de moral, pois "Num sentido jurídico-positivo, fonte do Direito só pode ser o Direito." (KELSEN, 2001)[48]. Finalmente, o problema da eficácia considera caráter histórico e sociológico das normas, que leva ao desenvolvimento da sociologia do direito.

As dimensões deontológica, ontológica e fenomenológica propostas por Bobbio podem ser percebidas na citação de DIDIER (2015)[49] a Humberto Ávila sobre a proteção da confiança, que se irradia de fato jurídico com os seguintes elementos (grifo meu):

> **(1) base da confiança**, que é um ato normativo qualquer, que fundamenta um comportamento individual ou social;

[48] KELSEN, H., **Teoria pura do Direito**, 6ª ed, Ed. Martins Fontes, São Paulo,1998, p. 162.

[49] DIDIER JR., F. **Curso de direito processual civil: introdução ao direito processual civil, parte geral e processo de conhecimento, vol. I**, 17a ed., Ed. Jus Podivm, 2015, p. 141.

> **(2) confiança nessa base:** que delimita as expectativas de conhecimento e cumprimento de um direito ou dever;
> **(3) exercício da confiança:** que ocorre quando um sujeito atua com base no cumprimento futuro, positivo ou negativo, da norma;
> **(4) frustração por ato posterior do Poder Público**: que é a proteção do direito do sujeito ante a ação de terceiros, baseada na norma: qualquer ação contrária à norma pode ser considerada ilícita.

Novamente, esses elementos também podem ser traduzidos em **aspectos objetivos e subjetivos** (BRAGA, 2015)[50]. O primeiro diz respeito à estabilidade do sistema jurídico e os atos nele praticados; o segundo, às expectativas dos cidadãos em relação ao Estado – desse último, deriva-se o "princípio da confiança legítima", que diz respeito às relações entre privados e está amplamente ligado ao princípio da boa-fé, que também tem aspectos objetivos, relacionados à lealdade e à conduta dos indivíduos, e subjetivos, relativos aos valores individuais.

Ressalte-se que a boa-fé e a segurança jurídica têm caráter universal: CLAES *et al* (2009)[51] afirma que a segurança jurídica é um conceito jurídico estabelecido tanto nos sistemas jurídicos de direito civil quanto na *common law*. Na tradição do direito civil, a segurança jurídica é definida em termos de máxima previsibilidade do comportamento dos seus representantes e oficiais. Na tradição do direito consuetudinário, a certeza jurídica é frequentemente explicada em termos da capacidade dos cidadãos para organizar os seus negócios de tal maneira que não infringem a Lei. Em ambas as tradições jurídicas, a segurança jurídica é considerada um valor de base para a legalidade das medidas legislativas e administrativas tomadas pelas autoridades públicas. O intuito é garantir que exista a confiança entre as partes sem que haja qualquer tipo de relacionamento prévio e garantir que alguma autoridade, ainda que apenas escolhida pelas partes para apenas um ato, garanta a correição das informações e o equilíbrio entre as partes para uma transação específica mediante o uso de seus registros.

Conforme coloca ARAÚJO(2009)[52], entre Poderes e instituições, a confiança tem ainda mais relevância:

> O princípio da proteção da confiança pode provocar sérias objeções quando manejado de uma forma que impeça o pleno exercício de qualquer das funções estatais. Quando empregado para proteger o particular diante de atos

[50] BRAGA, B. C. M. **Os princípios da segurança jurídica, confiança legítima e boa-fé: breves notas distintivas**, 2014, disponível para consulta pública em <https://bit.ly/2Ioewwu>, consultado em 11/09/2018.
[51] CLAES, E., KROLIKOWSKI, M , **Facing the Limits of the Law**, Springer Science & Business Media, Apr 21, 2009, p. 92-93.
[52] ARAÚJO, V. S. **O princípio da proteção da confiança: uma nova forma de tutela do cidadão diante do Estado**, Ed. Impetus, 2009, p. 165.

> legislativos, o princípio acaba interferindo na liberdade de configuração política desse poder. Em face do administrador público, ele demanda uma revisão no exercício da sua discricionariedade. E, quando atua em relação aos atos jurisdicionais, a proteção da confiança pode ameaçar a independência do magistrado. Não é possível, do ponto de vista teórico e prático, estudar e aplicar o princípio da proteção da confiança uniformemente em relação a todos os tipos de manifestação do poder estatal. Cada uma das funções primordiais dos poderes republicanos é capaz de criar e frustrar a confiança do particular de uma maneira específica. Cada poder tem feições próprias. Aliás, isso tem relação direta com o fato de cada poder estatal dirigir sua atenção primordialmente para um determinado momento temporal. Usualmente, o Poder Legislativo se ocupa do futuro, o Executivo se volta para o presente, enquanto que o Judiciário se preocupa com o passado.

Os princípios supracitados necessitam ser instrumentalizados para que se aperfeiçoem. TARTUCE(2018)[53] coloca que as formalidades exigidas pela Lei têm por finalidade a garantia de autenticidade de negócios jurídicos, para, eventualmente, facilitar sua prova e garantir a preservação da autonomia privada, objetivando sempre a certeza e a segurança jurídica. LOUREIRO(2015)[54] enfatiza a necessidade de certeza e publicidade de situações jurídicas. É possível dizer que essa segurança se materializa na boa-fé objetiva existente entre as partes que participam de um negócio e nas instituições encarregadas na manutenção e evolução do sistema jurisdicional, o que inclui a criação e preservação de registros de maneira neutra e sistematizada.

Contudo, a noção de soberania do Estado e o alcance da jurisdição fica esvanecida quando não há fronteiras físicas bem definidas ou qualquer tipo de autoridade central a quem se recorrer.

5. VALIDADE DA NORMA NO CIBERESPAÇO

ALEXY(2011)[55] fala de três dimensões distintas e complementares entre si para definir a validade de uma norma: eficácia social, correção material e legalidade com o ordenamento, que leva aos conceitos sociológico, ético e jurídico, respectivamente.

O objeto sociológico de uma norma é sua validade social, que ocorre quando a norma é observada ou quando sua não observância é punida. Essa punição (em consequência, sua validade), é relativizada dentro do sistema normativo e dos costumes sociais, o que leva à derivação de "graus de validade", de sua relativização conforme o caso concreto observado. Pode incluir a coação física legítima, organizada pelo Estado, em que a punibilidade advinda

[53] TARTUCE, F., **Manual de direito civil: volume único** 7ª ed., Ed. Método, 2017, p. 165.
[54] LOUREIRO, L. G., **Registros Públicos -Teoria e Pratica**, 8ª ed., Editora Jus Podivm, 2017, p. 52.
[55] ALEXY, R., **Conceito e Validade do Direito**, 1ª ed., São Paulo, Editora Martins Fontes, 2011, p. 101 a 112.

da norma deve ser suficientemente ampla para admitir não apenas a materialização de determinada conduta, mas também seu *animus*, sua intencionalidade.

Isso leva em consideração também o campo moral, em que a validade de uma norma delimita sua dimensão ética, que subjaz simultaneamente teorias do direito natural e racional, independentemente de sua eficácia social ou legalidade perante o ordenamento jurídico.

Em contraste, a validade jurídica pressupõe tanto a eficácia social quanto de sua promulgação por órgão competente: engloba tanto aspectos positivistas quanto não positivistas. Isso cria problemas de ordem interna e externa. Nesse sentido, ALEXY(2011, p. 110) questiona o positivismo jurídico de Hans Kelsen: o Direito não é a única fonte do Direito, mas, de maneira circular, a norma jurídica deriva sua validade numa norma fundamental. Em suas palavras, (Normas) *Perdem sua validade jurídica quando são extremamente injustas. Sua validade carece de um mínimo de justificabilidade moral que, ainda que mínima, seja reconhecida.*

Num espaço geográfico delimitado e num determinado tempo, pode-se dizer que uma ordem jurídica é válida se suas normas são globalmente eficazes, ou seja, se são observadas e aplicadas, sob o risco de ocorrer "desuetudo" (caducidade, perda de utilidade no contexto em que se insere): a prática que anula uma norma existente, o que significa dizer que o Direito necessita de reforço, de algum poder coercitivo. Essa afirmação traz a imagem do poder coercivo que a Lei tradicionalmente exerce. Porém, nas últimas décadas, as delimitações de jurisdição, hierarquia e poder têm mudado: com o desenvolvimento do "ciberespaço", um mundo virtual criado pelas tecnologias da informação e comunicações que abre a possibilidade para que indivíduos possam se comunicar, oferecer serviços e praticar comércio - e também crimes - com muito pouca ou sem nenhuma regulação até o dado momento. De maneira mais completa, MAYER *et al* (2014)[56] traz a seguinte definição:

> O ciberespaço é um domínio global e dinâmico (sujeito a constantes mudanças) caracterizado pelo uso combinado de elétrons e espectro eletromagnético, cujo objetivo é criar, armazenar, modificar, trocar, compartilhar, extrair, usar, eliminar informações e romper limites físicos.

[56] MAYER, M, MARTINO, L., MAZURIER, P., TZVETKOVA, G., **How do you define Cyberspace?**, Portal Academia, 19/05/2014, disponível em <https://bit.ly/2MHjSaV>, acesso em 11/10/219: "Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources. Cyberspace includes: a) physical infrastructures and telecommunications devices that allow for the connection of technological and communication system networks, understood in the broadest sense (SCADA devices, smartphones/tablets, computers, servers, etc.);b) computer systems (see point a) and the related (sometimes embedded) software that guarantee the domain's basic operational functioning and connectivity; c) networks between computer systems; d) networks of networks that connect computer systems (the distinction between networks and networks of networks is mainly organizational);e) the access nodes of users and intermediaries routing nodes; f) constituent data (or resident data)."

> O ciberespaço inclui:
> a) infraestruturas físicas e dispositivos de telecomunicações que permitem a conexão de redes de sistemas tecnológicos e de comunicação, compreendidos no sentido mais amplo (dispositivos SCADA[57], *smartphones* / *tablets*, computadores, servidores, etc.);
> b) sistemas de computador e os softwares relacionados (às vezes incorporados) que garantem o funcionamento operacional básico e a conectividade do domínio;
> c) redes entre sistemas de computadores;
> d) redes de redes que conectam sistemas de computador (a distinção entre redes e redes de redes é principalmente organizacional);
> e) os nós de acesso de usuários e nós de roteamento de intermediários;
> f) dados constituintes (ou dados residentes).

LESSIG(1999)[58], em sua *pathetic dot theory*, fala de diferentes forças que que coexistem e moldam a ação dos indivíduos de maneira independente à sua vontade: a lei, que cria restrições artificiais, regulamentos que criam determinados comportamentos pela coação institucional e o risco da punição; normas sociais, que determinam os traços de determinada cultura e a pressão social para reforçar comportamentos; o mercado, que incentiva ou desencoraja ações específicas por meio do mecanismo de oferta e demanda; e a arquitetura, as características do mundo que impõem restrições de qualquer natureza: biológica, tecnológica, geográfica, entre outras.

No que toca às arquiteturas tecnológicas que compõem o ciberespaço, é possível criar redes que coíbam ações e imponham fluxos de informação: quem define políticas nesse espaço, o faz mediante a escolha de regras de fluxo, feitas por configurações. O *design* dos protocolos de rede e aplicações pode criar regulações bastante efetivas: a aplicação da lei é *ex ante* e determinística. Mas a determinação desse *design* pode não ter qualquer tipo de correlação com a lei vigente no "mundo real". Ao se tratar de Direito e tecnologia em sentido amplo, especialmente quando se trata de internet, há uma grande área a ser explorada. DE FILIPPI(2016)[59] comenta que

> Direito e tecnologia desfrutam de um relacionamento complicado e, em grande parte, interconectado. Por um lado, o Estado está lutando para exercer sua soberania sobre a Internet, regulando o código para (indiretamente) regular usuários individuais. Por outro lado, o código é cada vez mais

[57] SCADA - Supervisory Control and Data Acquisition - Controle de supervisão e aquisição de dados, normalmente usados em sistemas de telemetria e automação.
[58] LESSIG, L., **Code and Other Laws of Cyberspace**, Ed. Basic Books, 1999
[59] DE FILIPPI, P., HASSAN, S, **Blockchain Technology as a Regulatory Technology From Code is Law to Law is Code**, First Monday, Volume 21, Number 12 - 5 December 2016, p. 5: "Law and technology enjoy a complicated, and to a large extent interconnected, relationship. On the one hand, the State is struggling to exercise its sovereignty over the Internet, by regulating code in order to (indirectly) regulate individual users. On the other hand, code is increasingly employed in a wide variety of sectors to regulate behaviors — either jointly with, or in addition to, existing laws."

> empregado em uma ampla variedade de setores para regular comportamentos - em conjunto ou em complemento às leis existentes.

No intuito de traduzir os parâmetros que limitam as leis, REIDENBERG(1998)[60] propõe uma comparação entre que determinadas dimensões de um ordenamento jurídico do mundo real e suas equivalências no ciberespaço, a que ele chama de "Lex Informatica":

Figura 4: Correspondência entre a regulação legal e a *Lex Informatica*

	Legal Regulation	Lex Informatica
Framework	Law	Architecture standards
Jurisdiction	Physical Territory	Network
Content	Statutory/Court Expression	Technical Capabilities Customary Practice
Source	State	Technologists
Customized Rules	Contract	Configuration
Customization Process	Low Cost Moderate cost standard form High cost negotiation	Off-the-shelf configuration Installable configuration User choice
Primary Enforcement	Court	Automated, Self-execution

Fonte: REIDENBERG, J., Lex Informatica, 1998, p. 569

Essencialmente, a tabela mostra os análogos para os principais elementos de um regime legal. A base do regime legal são as leis, criadas e mantidas por uma autoridade constituída e legitimada num certo território e tempo. Para os sistemas em geral, com especial ênfase nos informáticos, os padrões arquiteturais são os definidores da estrutura básica para o comportamento de usuários e para os padrões dos fluxos de informações nos limites de uma rede: são os protocolos e sistemas de informação.

[60]REIDENBERG, J. R., **Lex Informatica: The Formulation of Information Policy Rules Through Tecnology**, Texas Law Review, vol. 76, n. 3, February 1998, disponível em <https://bit.ly/2lOJkjB>, acesso em 12/09/2019.

REIDENBERG(1996) enfatiza que há sobreposição entre a lei e as redes. Enquanto um regime jurídico se aplica nos limites de um território bem definido, em que há um estado soberano para exercer seu poder, os sistemas e redes de comunicação não têm tal dependência, pois seus limites são definidos pelas características da própria rede. Porém, seus usuários estão sob a jurisdição do local onde se encontram fisicamente.

O conteúdo das leis advém de uma linguagem estatutária e pela interpretação institucional, definida pelos agentes do Estado e válida dentro de sua jurisdição. Por exemplo, os contratos privados são utilizados para personalizar o relacionamento entre partes em conformidade com os limites regulamentados na lei, admitindo podem ocorrer situações em que sua aplicação não é possível, em que a lei é inválida.

Nos sistemas informáticos, o regramento é dado pelo código que programa seus diferentes componentes. O código é criado por desenvolvedores, que podem ou não observar os ditames legais de onde vivem. O código não é neutro: ele pode esconder em si as crenças daqueles que o construíram. Mais ainda, quando se fala de sistemas estatísticos adaptativos (base para diversas aplicações do que se chama hoje de "inteligência artificial"), o próprio uso dos recursos dos sistemas faz com que o próprio comportamento do sistema se adapte ao comportamento dos seus usuários, que podem ignorar qualquer tipo de observância aos regramentos vigentes, legais ou morais. Não há simetria entre as partes: a relação imposta pelo código, que é criado pelos desenvolvedores.

Nas situações em que é oferecido aos usuários a oportunidade de customizar sua experiência, isso ocorre dentro dos limites da arquitetura: diferente das leis tradicionais, em que sua aplicação ocorre *a posteriori*, perante tribunais, as regras dos sistemas são aplicadas *ex ante*, no momento em que o usuário começa a utilizá-lo ou a fazer parte de uma determinada rede.

Ainda que exista independência entre as esferas do direito e da tecnologia, elas interagem e se influenciam, o que gera uma relação complexa de construção de utilidade e confiança, de interdependências, que moldam a relação entre indivíduos e instituições, em diferentes graus. DE FILIPPI(2016)[61] destaca a evolução desse relacionamento nas últimas décadas, que os atores do Direito e os Reguladores em geral constroem cada vez mais confiança em novas ferramentas, visto estarem imersos em inovações tecnológicas, de dependerem dos recursos tecnológicos em seu cotidiano.

[61] DE FILIPPI, P., HASSAN, S, **Blockchain Technology as a Regulatory Technology From Code is Law to Law is Code**, First Monday, Volume 21, Number 12 - 5 December 2016, p. 1-5

A autora afirma que diferentes fases podem ser observadas na inserção e amalgamação da tecnologia. Primeiro, ocorre a digitalização pura e simples de informações, o que significa sua disponibilidade num novo suporte; segundo, processos de decisão são automatizados: desde cálculos e referências científicas até pesquisas e comparações jurisprudenciais são passíveis de automação; terceiro, regras legais passam a ser incorporadas nos códigos-fonte: trata-se de regras que precisam ser observadas *a priori*, de maneira que os sistemas estipulam o que pode ou não ser feito em seu domínio em conformidade com os regulamentos externos de maneira objetiva; e finalmente, a dependência crescente das tecnologias da informação e comunicações gera tamanha influência na criação de leis que, gradualmente, a regra legal se aproxima da norma técnica.

Entretanto, há diversos desafios para concretizar a última parte, com questões relevantes ainda em aberto. A interpretação de conceitos como propriedade, identidade e segurança é particularmente sensível. Para uma quantidade significativa desses casos, Tecnologias de Registro Distribuído (*Distributed Ledger Technologies* - DLT), com destaque, o *Blockchain*, têm sido consideradas promissoras formas de solução[62].

6. NADA NOVO DEBAIXO DO CÉU: TECNOLOGIAS DE REGISTRO DISTRIBUÍDO

Sistemas de processamento distribuído foram comuns na década de 1970, até a popularização dos computadores pessoais. Tecnicamente, além das estruturas físicas, sistemas podem compartilhar memória, processamento e registros em estruturas de dados específicas. Sua comunicação e gerenciamento são realizados pelo uso de protocolos específicos, com ou sem a presença de uma unidade central.

Para registros compartilhados, é necessário que exista um protocolo que tenha a capacidade de coordenar a relação entre os diferentes participantes, que saiba exatamente onde cada parte do registro se encontra, e consiga controlar o que cada usuário tem direito a ler, alterar ou gravar sobre determinado registro e em que tempo é possível realizar tais ações. É

[62]VOS, J., **Blockchain based land registry: panacea, illusion or something in between?**, ELRA, 7th annual encounter, 2017, disponível em <https://bit.ly/2m2lC3w>, acesso em 11/09/2019.

necessário que existam mecanismos capazes de garantir a integridade dos registros, a fim de preservar, no mínimo, sua exatidão.

Quando se fala em *blockchain*, é comum que a imprensa se refira à tecnologia que sustenta o Bitcoin, destacando sua imutabilidade, isto é, uma vez que dados são inseridos numa corrente, não seria mais possível alterá-los. Outra característica importante é a transparência, oriunda da possibilidade de que todos os participantes tenham acesso a todas as transações registradas na corrente. Colabora com esta característica a descentralização do processamento das transações, que ocorre entre os pares da rede que possuem uma cópia dos registros: quanto mais cópias da base de dados existirem, mais robusto e transparente será o sistema. É necessário entender um pouco melhor essas características para que se possa compreender a aplicabilidade e relevância desta tecnologia.

Embora a definição detalhada do que é um "blockchain" ainda esteja em debate na comunidade, é necessário reconhecer que um *blockchain* é um (ou parte de um)"Sistema de informação"[63], cujo conceito é relativamente amplo.

Tratando especificamente de TIC, é possível afirmar que cada forma particular de organizar dados de forma lógica em um sistema computacional eletrônico é chamada de "estrutura de dados". Estas estruturas guardam estados físicos (por exemplo, ligado ou desligado, carregado com uma carga negativa ou positiva, com ou sem voltagem) que, mediante o uso de protocolos e códigos específicos, equivalem a dados guardados diretamente em espaços contínuos de memória (o suporte que permite a persistência dos estados físicos conhecidos) ou por "ponteiros", que são referências indiretas a outros espaços de memória (PATEL, 2009).[64]

Conforme o problema a ser resolvido, os tipos de estrutura de dados podem se combinar e criar outros subtipos para realizar operações com seus elementos. Dentre essas operações, podemos citar buscas, organização, inserção, retirada e assim por diante.

---

[63] Trata-se de métodos para armazenar, organizar, manter e recuperar dados de maneira eficiente, independentemente do suporte, ou seja, que podem ser executados de diferentes maneiras, variando conforme o contexto de aplicação e tecnologias disponíveis.

[64]PATEL, J, **Data Structure, Algorithms and Design Techniques**, 2009, disponível em <https://bit.ly/2lBATbk>, acessado em 07/09/2019. "Data may be organized in many different ways: the logical or mathematical model or a particular organization of data is called a data structure." Data structures are classified either linear or nonlinear. A data structure is said to be linear if its elements form a sequence, or, in other words, a linear list. There are two ways of representing such structures in memory. On way is to have the linear relationship between the elements represented by means of sequential memory locations. These linear structures are called arrays. The other way is to have the linear relationship between the elements represented by means of pointers or links. These linear structures are called linked lists. (…) Exemples to non-linear structures are trees and graphs. We may perform the following operations on any linear structure, whether it is an array or a linked list.

De maneira geral, o que se chama de "blockchain" funciona como uma estrutura de dados não-linear baseada em árvores de Merkle[65]. Neste tipo de estrutura, um bloco sempre referencia o anterior, formando um conjunto de registros em que qualquer modificação faz com que todos os resultados se modifiquem (vide Anexo C). Como demonstrado anteriormente, termo ganhou popularidade com o artigo que marca o nascimento do Bitcoin[66], em 2008.

Utiliza-se largamente elementos de criptografia, tanto simétrica quanto assimétrica, *hashes* matemáticos, árvores de Merkle e algoritmos de construção de consenso, para garantir a coesão e a integridade na criação, sequenciamento e manutenção de blocos de registros, que comporão um banco de dados compartilhado e suficientemente seguro para que se possam fazer transações de valores.

Nesse tipo de banco de dados, os registros relacionam-se fortemente entre si. Na formação dos blocos, diversas operações são executadas com a finalidade de organizar, manter e recuperar cada registro[67].

Os blocos contêm não apenas informações relativas ao seu conteúdo (*payload*), mas também uma referência matemática unívoca ao bloco precedente e informações de data e hora de sua formação. Em outras palavras, a modificação num bloco obrigaria o recálculo de todos os blocos subsequentes (vide Anexo C e F).

A referência matemática unívoca feita por funções *hash* é o componente fundamental para a formação dos *blockchains*: é possível produzir identificações únicas e padronizadas para qualquer quantidade de dados com um esforço computacional relativamente baixo. Isso significa que é fácil verificar a autenticidade de um conjunto de dados a partir de seu *hash*. Qualquer modificação na entrada de dados gera uma saída completamente diferente. Em contraste, a dificuldade de se encontrar um código completo desconhecido a partir de um *hash* é enorme. Na prática e para fins legais, esses códigos funcionam como garantia de integridade (explicação completa nos Anexo A e B).

No caso específico do *blockchain* do Bitcoin, é possível afirmar que sua grande parte de sua solidez esteja no uso dos algoritmos de consenso e na absoluta transparência que as bases de dados de registro distribuído permitem.

---

[65]Estrutrua criada por Ralph Merkle em 1979, sob a patente US4309569A, disponível em <https://bit.ly/33Asw0U>, acesso em 13/09/2019.

[66]O artigo "Bitcoin: A Peer-to-Peer Electronic Cash System", de um autor que se denomina "Satoshi Nakamoto", marca o nascimento do Bitcoin, uma rede que utiliza "blockchain" como tecnologia para o registro de transações. Disponível na íntegra em <https://bitcoin.org/bitcoin.pdf>, acesso em 11/09/2019.

[67] WEGNER, P., REILLY, E. D., **Encyclopedia of Computer Science**. UK: John Wiley and Sons, 2003, pgs. 507 a 512, tradução livre.

> Bitcoin ou outra moeda digital não é salva em um arquivo em algum lugar; é representado por transações registradas em uma cadeia de blocos - como uma planilha ou livro-razão global, que aproveita os recursos de uma grande rede P2P para verificar e aprovar cada transação Bitcoin. Cada *blockchain*, como o do Bitcoin, é distribuído: é executado em computadores fornecidos por voluntários em todo o mundo. Não há banco de dados central para hackear. O blockchain é público: qualquer um pode vê-lo a qualquer momento, porque reside na rede ... e o blockchain é criptografado ... usa chaves públicas e privadas (como um sistema de duas chaves para acessar um cofre) para manter a segurança virtual. (TAPSCOTT, 2016, tradução livre)[68]

Os algoritmos de construção de consenso permitem que membros de uma rede validem um bloco de dados antes que ele seja inserido definitivamente numa cadeia. Especialmente numa rede aberta, pode não ser necessário que exista qualquer conhecimento prévio ou relação de confiança pré-estabelecida entre os nós participantes (por exemplo, no caso de *proof-of-work*, é necessário que os participantes concordem na solução de um problema de difícil resolução com base nos dados que estão validando). Cada um dos nós participantes pode ter uma cópia integral de todos os blocos válidos numa cadeia, formando um livro razão compartilhado. Portanto, o termo *Distributed Ledger* (Livro Razão Distribuído) ou simplesmente "DL".

É possível afirmar que tecnologias para a criação e manutenção de DLs (ou DLTs - *Distributed Ledger Technologies*) ainda estão em estágio inicial, mas a popularidade alcançada pelo Bitcoin mostrou que a ideia de registros descentralizados, autogeridos e autoexecutados, tem enorme potencial de aplicação (vide Figura 1): do rastreamento de mercadorias a transações monetárias ou títulos de propriedade, qualquer tipo transação ou registro que precise manter algum rastro nas diversas fases entre a origem e o destino.

Embora "blockchain" remeta imediatamente ao modelo de manutenção de registros do Bitcoin, a WEF lista três tipos de DLT viáveis: sistemas públicos sem permissão (como o Bitcoin), privados e autorizados e sistemas híbridos, com uso extenso de criptografia garantir minimamente o controle de autorização, autenticidade e responsabilidade nas transações. Cada um desses modelos é adequado para diferentes requisitos e finalidades, com diferentes formas de controle e acesso aos membros.

---

[68] TAPSCOTT, D., TAPSCOTT, A, **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**, Ed. Penguin, 2016: "Bitcoin or other digital currency isn't saved in a file somewhere; it's represented by transactions recorded in a blockchain—kind of like a global spreadsheet or ledger, which leverages the resources of a large P2P network to verify and approve each Bitcoin transaction. Each blockchain, like the [Bitcoin blockchain] is distributed: it runs on computers provided by volunteers around the world. There is no central database to hack. The blockchain is public: anyone can view it at any time because it resides on the network… and the blockchain is encrypted… it uses public and private keys (rather like a two-key system to access a safety deposit box) to maintain virtual security".

Figura 5: Tipos de Registro Distribuído

Fonte: WEF, disponível em <https://bit.ly/2HoLWL2>, acesso em 01/09/2019

Em sistemas de compartilhamento públicos e sem permissão, o acesso é garantido a qualquer indivíduo que queira participar na rede para extrair informações e gravar novos dados. Não há um proprietário único: a cada membro, é facultado ter uma cópia idêntica de todos os registros. Conforme dito antes, é o modelo do Bitcoin, que tem o objetivo de operar em um ambiente completamente aberto, resiliente a atores potencialmente mal-intencionados sem a necessidade de ponto central de confiança.

Nos sistemas públicos e com permissão, há um caráter híbrido: o acesso e permissionamento é concedido *ex ante,* mas todas as transações podem ser visíveis publicamente. As aplicações governamentais seriam um exemplo, pois apenas certas pessoas devem ter o poder de gravar novos dados na rede, mas todas as transações podem ser verificadas por qualquer pessoa.

O modelo mais fechado de sistema compartilhado é o privado e com permissão, em que apenas os que têm as devidas permissões podem gravar ou consultar dados. Não há restrição se o sistema tem um ou muitos proprietários.

Em redes baseadas em DLTs em que não existe hierarquia entre os membros, é necessário criar mecanismos que tenham capacidade de aferir a validade e a consistência das informações inseridas de maneira transparente, garantida por todos os nós da rede. Que exista integridade do histórico e evolução, com o objetivo de tornar as informações resistentes a adulterações, além de resiliência contra diversos tipos de ataques.

Essas características, porém, têm *trade-offs* tanto de natureza técnica quanto legal. Dentre os problemas de natureza técnica, é possível destacar o tempo de processamento de uma

transação, que é um impedimento para a adoção do grande público, ou o consumo de energia para a resolução problemas de *proof-of-work,* que podem tornar o custo de processamento dos blocos impeditivo. No que tange à natureza legal, é possível destacar as questões de transparência e privacidade, especialmente quando são armazenados dados pessoais ou sensíveis.

Nessa perspectiva, KUMAR *et al* (2014)[69] destaca que as leis sobre os fluxos de dados, sobre privacidade dos dados e dos proprietários diferem significativamente quando as fronteiras políticas são ultrapassadas, o que pode levar a perspectivas conflitantes. Leis como a LGPD e o RGPD, por exemplo, trazem definições próprias bastante próximas do que são dados pessoais e o que são dados sensíveis.

Embora as questões de segurança da informação como confidencialidade, integridade e autenticidade sejam resolvidas com o uso de técnicas de criptografia, FINCK(2018)[70] considera que, para fins de RGPD, dados criptografados são uma forma de "pseudoanonimização", não de anonimização, uma vez que o titular dos dados é ainda passível de identificação por meios indiretos, e conclui que dados pessoais, sejam eles criptografados ou sujeitos a um processo de *hash*, continuam sendo dados pessoais sob a definição do RGPD.

7. BLOCKCHAIN E O DIREITO

Ao tratar de questões regulatórias na internet, REIDENBERG(1998) lista três grandes problemas: (i) o tratamento do conteúdo, que tem a ver com questões como a responsabilidade de intermediários, com a legalidade do material oferecido e sua adequação para o público, haja vista a dificuldade de se controlar o teor de determinadas mídias e fluxos de dados; (ii) o tratamento de informações pessoais, que ganhou bastante publicidade com a discussão de estatutos como a LGPD no Brasil e o RGPD na União Europeia, e abrem espaço não apenas para crimes contra indivíduos em particular, mas também para abuso de autoridade e para a

[69]KUMAR, V, CHERJELA, B, MADRIA, S, MOHANIA, M, **A Survey of Trust and Trust Management in Cloud Computing,** em Managing trust in the Cyberspace, CRC Press, 2014, p. 47: "Laws regarding data, privacy of data, and privacy of data owners differ vastly when political boundaries are crossed, which results in conflicting perspectives in case of a contention. The proprietary nature of the clouds lends to their being non-transparent to outsiders. This makes evaluation of a cloud difficult from a trust management perspective. Lack of standards pertaining to security and performance in cloud computing also makes trust management a challenge."

[70]FINCK, M., **Blockchains and Data Protection in the European Union**, European Data Protection Law Review, Volume 4, Issue 1, p. 17 - 35, 2018, p. 23: "Encryption is considered a pseudonymisation technique under the EU data protection regime given that the data subject can still be indirectly identified so that it can, on its own, not be considered as an anonymisation technique. The conclusion that transactional data that has been encrypted remains personal data for the purposes of the GDPR is accordingly unavoidable. Transactional data that has been subject to a hashing process also qualifies as personal data under the GDPR."

manipulação de massas, como o ocorrido no escândalo da empresa Cambridge Analytica[71]; e (iii) a preservação dos direitos de propriedade, sobremaneira os de propriedade intelectual, que podem ser copiados, alterados, distribuídos e utilizados sem qualquer conhecimento ou anuência dos detentores dos direitos e sem qualquer tipo de fiscalização por parte das autoridades.

Na tentativa de resolver esses problemas, diversas soluções técnicas foram propostas ao longo dos anos, como filtros de conteúdo, diferentes mecanismos de criptografia e identificação, protocolos, rótulos de conteúdo, certificações institucionais, *frameworks* de segurança, entre inúmeros outros, com graus de sucesso distintos.

É possível afirmar que o grande diferencial do Bitcoin foi tratar com êxito uma questão crucial: dinheiro. A criação de um meio de troca transparente e independente de qualquer tipo de autoridade, ente central ou intermediário garantiu a credibilidade suficiente para que se examinasse a aplicabilidade da tecnologia, o Blockchain, a outras áreas.

Tradicionalmente, os negócios e serviços conduzidos pela internet necessitam de um terceiro confiável para estabelecer a comunicação entre indivíduos que não têm qualquer tipo de relacionamento anterior. Delega-se a esses terceiros a responsabilidade de garantir a veracidade da transação, a autenticidade das partes e a expectativa de conclusão do negócio. Esses terceiros são formas de "sistemas peritos", que assumem riscos ao executar suas atribuições, demandando algum tipo de pagamento em troca, como o que ocorre com instituições bancárias, cartões de crédito, seguradoras, autoridades certificadoras (vide Anexo E) e até mesmo os governos.

Potencialmente, a imutabilidade, transparência, irretrabilidade e rastreabilidade esperadas de um sistema baseado em *blockchains* eliminam a necessidade intermediários, dado que estabelecem relações diretas entre as partes envolvidas em uma transação, com a confiança garantida pelo próprio funcionamento da rede. Nesse sentido, DE FILIPPI(2016)[72] afirma que

> Ao alavancar a transparência e a imutabilidade das tecnologias *blockchain*, é possível restaurar a unicidade e a transferibilidade das obras digitais, vinculando cada cópia digital a um *token* específico no *blockchain*. Os autores podem associar esses *tokens* a um conjunto específico de direitos sobre suas obras digitais e negociá-los da mesma maneira que trocariam *tokens* digitais.

[71] THE NEW YORK TIMES, **Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens**, 19/03/2018, disponível em <https://nyti.ms/2mOCACK>, consultado em 24/09/2019.

[72] DE FILIPPI, P., HASSAN, S, **Blockchain Technology as a Regulatory Technology From Code is Law to Law is Code**, First Monday, Volume 21, Number 12 - 5 December 2016: "By leveraging on the transparency and immutability of blockchain technologies, it is possible to restore the unicity and transferability of digital works, by linking every digital copy to a particular token on the blockchain. Authors can then associate these tokens with a particular set of rights to their digital works and trade them in the same way as they would trade digital tokens."

O corolário é que **sistemas baseados em *blockchains* criam uma "escassez artificial"**[73] no meio digital: uma vez que ações são registradas, que um *smart contract*[74]cumpre seus efeitos, que uma transação ocorre, a expectativa é que a ação seja irreversível. Isso permite a transferência automática de propriedade com algum valor atribuído no mundo real, a emissão de documentos digitais por autoridades competentes e passíveis de validação pela internet, a proteção de direitos autorais sobre uma obra artística ou científica ou qualquer outro tipo de ativo digital: bilhetes de cinema, passagens aéreas, *vouchers* de serviços. Potencialmente, também mandados judiciais, evidências num processo e votos numa eleição. Porém, com pouco espaço para princípios consagrados como o contraditório e a ampla defesa.

Tratando especificamente de Direito dos Contratos, há uma riqueza enorme de questões a serem exploradas, que vão desde a interpretação da lei até o cumprimento de medidas judiciais e extrajudicial. A própria palavra "Contrato", segundo GARNER(2001, tradução livre)[75], já enseja diversas interpretações:

> 1. Um acordo entre duas ou mais partes que cria obrigações que são executórias ou reconhecíveis por lei.
> 2. Os escritos que estabelecem tal acordo […].
> 3. Vagamente, um acordo inexequível entre duas ou mais partes para fazer ou não fazer uma coisa ou conjunto de coisas [...].
> 4. Uma promessa ou conjunto de promessas por uma parte de uma transação, executória ou de outra forma reconhecível por lei; a escrita que expressa essa promessa ou conjunto de promessas [...].
> 5. De maneira geral, qualquer dever legal ou conjunto de deveres não impostos pela lei do delito; esp., um dever criado por um decreto ou declaração de um tribunal […].
> 6. O corpo da lei que trata de acordos e trocas.

---

[73] O'DWYER, R, **Limited Edition: Producing Artificial Scarcity For Digital Art On The Blockchain And Its Implications for The Cultural Industries**, 2018, dispovível em <https://bit.ly/2lx8dAt>, consultado em 24/09/2019.

[74] FAIRFIELD, J., **Smart contracts, Bitcoin bots, and consumer protection.** Wash. & Lee L. Rev. Online 71, 2104, 35-299, disponível em <https://bit.ly/2njxBue>, acesso em 11/09/2019, pg. 38: "It's important to understand how extensive the scope of "contract" and "contract law" is, because it provides context for evaluating the potential risks and benefits of blockchain-based "smart contracts." Smart contracts are "automated programs that transfer digital assets within the block-chain upon certain triggering conditions".

[75] GARNER, B. A., **A dictionary of modern legal usage**. Oxford University Press, USA, 2001, p. 259:
"1. An agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law .
2. The writing that sets forth such an agreement […].
3. Loosely, an unenforceable agreement between two or more parties to do or not do a thing or set of things; a compact […].
4. A promise or set of promises by a party to a transaction, enforceable or otherwise recognizable at law; the writing expressing that promise or set of promises […].
5. Broadly, any legal duty or set of duties not imposed by the law of tort; esp., a duty created by a decree or declaration of a court […].
6. The body of law dealing with agreements and exchange.
7. The terms of an agreement, or any particular term"

7. Os termos de um contrato ou qualquer termo específico

WERBACH *et al* (2017)[76] nos chama a atenção que "apesar dos grandes avanços no aprendizado de máquina, os computadores não têm o grau de entendimento sutil contextual, específico de domínio, necessário para resolver a ambiguidade contratual". É comum que a linguagem usada nas normas jurídicas seja deliberadamente vaga em nome de sua abrangência (POSCHER, 2011)[77]. No desenho de *smart contracts* ou qualquer artifício baseado em código, há pouco espaço para ambiguidade e, portanto, para a arbitragem judicial. DE FILLIPI(2016)[78] sedimenta este pensamento ao afirmar que

> A lei é intencionalmente ambígua, para que possa ser aplicada com mais facilidade caso a caso. É a sobreposição de múltiplas disposições legais, que cria uma sólida estrutura regulatória, com múltiplas limitações e exceções, a fim de acomodar a complexidade e a imprevisibilidade da sociedade humana.

É possível afirmar que a característica mais importante dos *blockchains* para o direito é sua expectativa de imutabilidade: não há outra característica que seja mais relevante nesta tecnologia em comparação com outras. Dito isso, o sucesso do projeto, construção e implementação de um sistema baseado em algum DLT depende muito do conhecimento e maturidade acerca do objeto do sistema a ser construído. Maturidade, neste contexto, significa ter uma visão bastante clara do que se pretende obter com um determinado sistema, com atenção aos pressupostos e implicações em esferas como as de negócio, direito e tecnologia. Cada uma dessas esferas tem riscos próprios, vulnerabilidades e peculiaridades acerca de seu funcionamento. Por exemplo, o que aconteceria se um *blockchain* para controle da propriedade de imóveis numa determinada região fosse dominado por um único indivíduo ou grupo? E se tal dominação levasse anos para ser descoberta? E se algum terceiro mal-intencionado conseguisse burlar os mecanismos de proteção existentes e tornasse os dados de toda a corrente

---

[76] WERBACH, K., CORNELL, N., **Contracts Ex Machina**, Duke Law Journal, 67, 2017, p. 366: "Despite great advances in machine learning, computers do not have the degree of contextual, domain-specific, subtle understanding required to resolve contractual ambiguity. "

[77] POSCHER, R., **Ambiguity and Vagueness in Legal Interpretation**, 2011, disponível em <https://bit.ly/2myyYVC>, consultado em 24/09/2019, p. 37: "Leaving the dubious and also more exceptional virtues aside, it seems mostly the reduction of decision costs that constitutes the value of vagueness. This value might also explain, why we find much more vague than precise general concepts in language and law. Both may often pay the price of vagueness for the use of more general"

[78] DE FILIPPI, P., HASSAN, S, **Blockchain Technology as a Regulatory Technology From Code is Law to Law is Code**, First Monday, Volume 21, Number 12 - 5 December 2016: "Law is intentionally ambiguous, so that it can be more easily applied on a case-by-case basis. It is the overlapping of multiple legal provisions, which creates a solid regulatory framework, with multiple limitations and exceptions in order to accommodate the complexity and unpredictability of human society"

inacessíveis? E se não houver controle rigoroso nos dados inseridos em cada bloco, que venha a ocasionar pedidos frequentes de alteração? A quem pedir providências caso isso ocorra?

Dentre os inúmeros riscos que se poderia elencar, o ponto que atualmente tem grande relevância é a privacidade, em seus mais diversos aspectos. Nos EUA (Estados Unidos da América), a discussão sobre a proteção da privacidade é antiga, e com frequência questiona-se a violação da 4ª Emenda[79] da Constituição Americana pelo uso indevido de dados, além de inúmeros casos judiciais e políticos sobre a liberdade de expressão. No Brasil, há vasta jurisprudência sobre o inciso X do Art. 5º da CF/88 e, mais recentemente, a promulgação da Lei Geral de Proteção de Dados e a expectativa de sua entrada em vigor geram apreensão tanto na iniciativa privada quanto na Administração Pública. Em termos de regulação estatal, é possível afirmar que a União Europeia se encontra em estágio de discussões mais avançado que o resto do mundo, dado que as discussões sobre o Regulamento Geral de Proteção de Dados abrangem uma quantidade razoável de países e sua discussão já se desenrola há vários anos.

8. PROTEÇÃO DA PRIVACIDADE: LIMITAÇÕES DE DLTs ANTE REGULAÇÃO PARA PROTEÇÃO DE DADOS

As DLTs são concebidas para processar cada transação de maneira descentralizada, deixando um arquivo contendo toda ou parte de sua base de dados em cada nó processador. No caso do Bitcoin, cada uma dessas bases contém dados dos usuários envolvidos em cada transação, o que permite rastrear todas as transações de uma determinada carteira por qualquer pessoa, mesmo que não participe da rede. A preservação de dados privados nesta situação não parece uma tarefa possível. Nesse sentido, FINCK(2018)[80], ao se referir ao RGPD, destaca que a maior parte das DLTs vista hoje em dia, em seu estado de desenvolvimento atual, não atenderia aos requerimentos específicos de proteção à segurança exigidos pelo estatuto.

---

[79] US Constitution, 4th Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Disponível em <https://constitution.findlaw.com/amendment4.html>, acesso em 11/09/2019.

[80] FINCK, M**., Blockchains and Data Protection in the European Union**, European Data Protection Law Review, Volume 4, Issue 1, 2018, p. 17: "In their current state DLT will in most, if not all, instances be incompatible with the GDPR as the specific requirements of the EU data protection framework cannot be easily applied to distributed ledgers"

DLTs fazem uso intenso de criptografia para garantir a privacidade dos conteúdos e a autenticação das partes nas transações. Porém, a criptografia é uma técnica de pseudonimização, uma vez que o titular dos dados ainda pode ser identificado indiretamente. Dito isso, para os fins do RGPD[81], a conclusão lógica é que que os **dados transacionais criptografados ou originados de algum processo de *hash* permanecem como dados pessoais**. Há implementações de *blockchain*, mais próximas ao apregoado pelo regime de proteção de dados, que meramente retêm na corrente a prova de que determinada transação é válida, enquanto os detalhes da transação são mantidos em algum local protegido.

No atual estado de entendimento sobre o assunto, as tentativas de regulação sobre sistemas de DLT exigiriam identificar se algum nó ou conjunto de nós participantes da rede se classificariam como *data controllers,* que teriam a capacidade de aplicar regras para a inserção de dados. Também seria necessário verificar se esses controladores estariam sujeitos a alguma legislação específica do local onde operam.

Quando não há nós que centralizem o controle da rede, como a maior parte das moedas criptográficas existentes, ou se não há jurisdição aplicável, então qualquer controle fica a cargo da própria rede, isto é, do código que a define, e a demanda de usuários pelos serviços oferecidos por esta rede – se não há usuários interessados, não há rede.

A regulação externa, portanto, é limitada. Para os casos em que é possível aplicar alguma regulação, a questão da privacidade merece especial atenção, pois, à primeira vista, representam o oposto do que as DLTs oferecem. Relativo a este tema, os trabalhos de Michèle Finck ao longo de 2018 analisam com profundidade o uso de *blockchains* à luz do RGPD. Ressalte-se que questões levantadas pela autora são também aplicáveis à legislação brasileira, dada a proximidade das normas.

Os pontos relevantes levantados pela autora e discutidos a seguir são: (i) Minimização de dados, (ii) o Direito ao Acesso, (iii) o Direito à Retificação e (iv) o Direito ao Esquecimento.

---

[81] ***Idem, Ibdem***, pg. 23: "Encryption is considered a pseudonymisation technique under the EU data protection regime given that the data subject can still be indirectly identified so that it can, on its own, not be considered as an anonymisation technique. The conclusion that transactional data that has been encrypted remains personal data for the purposes of the GDPR is accordingly unavoidable. Transactional data that has been subject to a hashing process also qualifies as personal data under the GDPR".

8.1. MINIMIZAÇÃO DE DADOS

O RGPD, em seu Art. 5[82], exige que os dados pessoais a serem coletados sejam específicos, explícitos, tenham finalidade legítima e não sejam utilizados posteriormente para fins diversos.

O princípio de minimização de dados refere-se a várias dimensões, começando pelo escopo e as categorias de dados coletados. Além disso, há também que se considerar a duração por qual os dados pessoais podem ser retidos, tendo em vista que um dos requisitos é que esses dados sejam excluídos após o uso pretendido.

Uma das implicações é que apenas os dados absolutamente necessários para a finalidade do controlador podem ser obtidos e processados. DLTs baseadas no Blockchain, porém, possuem duas características flagrantemente antagônicas à minimização de dados:

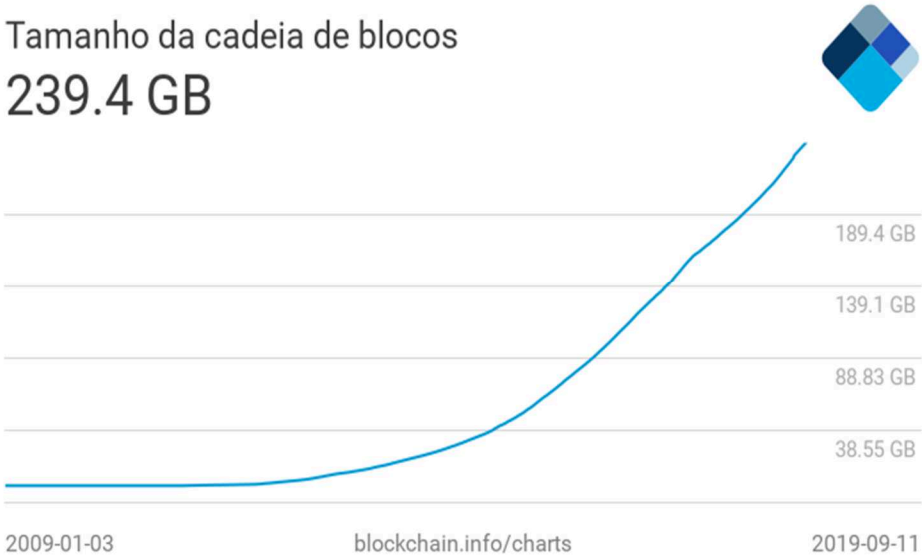
(i) são *append only*[83], o que significa que seus bancos de dados sempre crescem: pela natureza do seu funcionamento, uma vez inserido um dado, ele persiste indefinidamente, o que equivale a dizer que a cada bloco inserido, a cadeia aumenta enquanto houver quem os processe. A figura 6 ilustra o crescimento do *blockchain* do Bitcoin:

---

[82] RGPD, Art. 5, "1.Os dados pessoais são:
a)Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
b)Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»);
c)Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);
d)Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);
e)Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);
f)Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»)"

[83] FINCK, 2018, p. 28: "Data once added to a blockchain will perpetually remain part of the chain, given that it is an append-only database that continuously expands"

Figura 6: Crescimento do *blockchain* do Bitcoin.



Fonte: <https://bit.ly/2Kd1hlb>, acesso em 13/09/2019

(ii) em DLTs abertas, a informação completa é guardada em diversos nós, o que significa que mesmo os dados pessoais e sensíveis serão replicados.

Dados só poderiam ser removidos ou alterados em circunstâncias absolutamente extraordinárias, mesmo aqueles que já são obsoletos ou foram inseridos erroneamente.

Complementando este ponto, ZARSKY(2017)[84] afirma que:

> As justificativas para a minimização de dados são intuitivas e instrumentais. Quando o princípio de minimização é seguido, os controladores de dados têm menos oportunidades de prejudicar os direitos de proteção de dados dos titulares de dados. De fato, com menos dados, os controladores de dados não poderão ir além do uso consentido ou violar a privacidade de seus usuários de outras maneiras. Uma justificativa adicional pode estar relacionada ao domínio da segurança cibernética. Quanto mais tempo um controlador de dados reter informações pessoais (especialmente em grandes quantidades), maior o risco de esses dados serem invadidos por entidades internas e externas. O fato de os controladores de dados não terem incentivos suficientes

[84] ZARSKY, Z. T., **Incompatible: The GDPR in the Age of Big Data**, Seton Hall Law Review Vol. 47:995, 2017, p. 1009 e 1010, disponível em <https://bit.ly/2DEgcS>, acesso em 15/09/2019: "The justifications for data minimization are both intuitive and instrumental. When the minimization principle is followed, data controllers have fewer opportunities to undermine the data protection rights of data subjects. Indeed, with less data, data controllers will be unable to go beyond consented usage or violate their users' privacy in other ways. An additional justification can relate to the realm of cyber-security. The longer a data controller holds personal information (especially in large quantities), the greater the risk that such data would be hacked by both internal and external entities. The fact that data controllers do not have sufficient incentives to apply optimal cyber-security measures most likely enhances this risk of data leakage."

> para aplicar medidas ideais de segurança cibernética provavelmente aumenta esse risco de vazamento de dados.

FINCK(2019)[85] questiona se realmente há prejuízo do princípio da minimização de dados no uso de DLTs, considerando a vagueza do termo "dados adequados" na redação do artigo 5 (1)(c). Além disso, o Art. 39 afirma que os dados pessoais "só devem ser tratados se o objetivo do tratamento não puder ser razoavelmente cumprido por outros meios". Numa interpretação alternativa a este princípio, é possível dizer que a minimização não se refere tanto à quantidade de dados, mas à sua qualidade: a consequência prática é que a restrição ao processamento e guarda de dados pode depender de filtros de restrição por categoria, embora o Art. 25(2) exija que o administrador de dados implemente medidas técnicas e organizacionais apropriadas para garantir que, por padrão, apenas os dados pessoais necessários para cada finalidade específica do processamento são processados.

Essa obrigação se aplica à quantidade de dados pessoais coletados, à extensão de seu processamento, ao período de armazenamento e à acessibilidade. FINCK(2018)[86], semelhante a REIDENBERG(1998), propõe soluções técnicas para questões de Direito:

> Há, porém, soluções técnicas que podem vir a sanar essas dificuldades: dados transacionais ser armazenados e alterados fora do *blockchain*, dentro das limitações normativas a que estiverem vinculados, sem que necessariamente se altere o registro no bloco. Isso permitiria minimizar significativamente a quantidade de dados processada. Há exceções ao caso, como as chaves públicas mascaradas que não podem ser removidas retroativamente do registro. Existe uma situação semelhante em relação ao direito do RGPD de retificação.

8.2. O DIREITO DE RETIFICAÇÃO

O Art. 5º do RGPD exige que dados pessoais sejam precisos e "atualizados sempre que necessário". Tal previsão também existe no Art. 18[87] da LGPD. Caso seja realmente necessário

---

[85]FINCK, M., **Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?**, European Parliamentary Research Service, julho, 2019, p. 68, disponível em <https://bit.ly/2lxNLPE>, acesso em 09/09/2019.

[86] *Idem*, **Blockchains and Data Protection in the EU**, 2018: "A second look however reveals that technical solutions to these difficulties might be on the horizon. Transactional data that is stored off-chain can be modified and minimised in line with these legal requirements without touching the distributed ledger itself. The situation is however more difficult in relation to the pseudonymous public keys that cannot be retroactively removed from the ledger. A similar state of affairs exists in relation to the GDPR's right to amendment".

[87] BRASIL, LGPD, Lei nº 13.709/2018: "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: II - correção de dados incompletos, inexatos ou desatualizados;"

alterar registros, é preciso que existam instrumentos ou medidas capazes garantir sua correção, quer seja de maneira direta, pela alteração do registro, ou indireta, pela alteração da informação a que o registro na corrente referencia. WACHTER *et al* (2019, tradução livre)[88] destaca que

> A retificação depende implicitamente da noção de verificação, o que significa que um registro pode demonstrar ser inválido (ou seja, impreciso ou incompleto) e, portanto, 'corrigido' pelo titular dos dados. O direito é fácil de implementar quando os dados usados ou as inferências extraídas têm uma base factual ou, em outras palavras, são verificáveis (por exemplo, nome, data de nascimento, estado civil, renda). Para os dados fornecidos pelo titular, é possível recorrer a alguma forma de 'verdade da base' que demonstre a falha nos dados mantidos, seja a conta de eventos do titular dos dados, observações ou registros adicionais ou alguma outra informação.

No RGPD, esse direito é expresso no Art. 16,[89] cuja redação inclui dois pontos importantes: (i) a tempestividade das medidas, por um *periculum in mora* da manutenção de dados incorretos, portanto, uma solução deve ocorrer "sem demora injustificada"; e (ii) que informações suplementares podem ser utilizadas em situações em que os dados estejam incompletos.

Por padrão, DLTs são tipicamente construídos para tornar a exclusão e modificação de dados extraordinariamente onerosas, a fim de garantir a integridade, a confiabilidade e irretratabilidade dos dados inseridos na rede: há um flagrante contraste entre o dispositivo do RGPD segundo o qual dados sejam mutáveis para permitir seu apagamento ou, conforme exigido pelo Artigo 16, sua retificação.

Especificamente no caso de uma DLT aberta, a alteração dos dados pode depender não apenas de solicitação do titular de dados a todos os nós que participam da rede, mas também que eles disponham de mecanismos para atender à demanda. Cabe destacar que há situações

---

[88]WACHTER, S., MITTELSTADT, B, **A right to Reasonable Inferences: Re-thinking Data Protection Law in the age of Big Data and AI**, Columbia Business Law Review, 2019, disponível em <https://bit.ly/2VcrRzn>, acesso em 09/09/2019, p. 36: "Article 16 grants data subjects the right to rectify inaccurate personal data or complete incomplete data "by means of providing a supplementary statement" Rectification implicitly relies upon the notion of verification, meaning a record can demonstrably be shown to be invalid (i.e. inaccurate or incomplete), and thus 'corrected' by the data subject. The right is easy to implement when the data that is used or the inferences drawn has a factual basis or in other words is verifiable (e.g. name, date of birth, marital status, income). For data provided by the data subject, some form of 'ground truth' can be appealed to that demonstrates the flaw in the data held, be it the data subject's account of events, additional observations or records, or some other piece of information."

[89]UNIÃO EUROPEIA, RGPD, Art. 16, grifos meus: "O titular tem o direito de obter, **sem demora injustificada**, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de **uma declaração adicional**."

em que é impossível identificar todos os nós e, nas situações em que é possível, os nós não possuem instrumentos capazes de alterar dados armazenados num bloco.

À primeira vista, embora o exercício desse direito pareça ser impossível em *blockchains*, FINCK(2018) questiona se, nas situações em que for possível utilizar um registro suplementar para corrigir informações anteriores, ainda haveria atendimento à prerrogativa do Art. 16, uma vez que retifica dados futuros, todavia mantendo dados problemáticos, e propõe que dados transacionais sejam armazenados fora de *blockchains.*

Como consequência, haveria dados passíveis de serem alterados de acordo com os requisitos de proteção de dados sem que houvesse necessariamente modificação do *blockchain*. Esta medida pode facilitar a conformidade com o RGPD em relação aos dados transacionais, mas não a registros como chaves públicas (vide ANEXO A). Adicionalmente, o Art. 19 do RGPD também exige que o responsável pelo tratamento comunique qualquer retificação ou exclusão de dados pessoais a 'cada destinatário a quem os dados pessoais foram divulgados'.

8.3. O DIREITO DE ACESSO

O Direito de Acesso, de maneira quase simbólica, é o primeiro da lista dos direitos do titular[90], pois é pré-requisito para o exercício dos demais. A partir desse direito, permite-se ao titular entender quais dados estão sendo processados pelo controlador, o que normalmente é o primeiro passo necessário antes que qualquer outro direito possa ser exercido. Em outras palavras, o direito de acesso permite ao titular dos dados apontar que dados pessoais podem ser imprecisos, o que pode levá-lo a exercer seu direito à retificação nos termos do Artigo 16 do RGPD.

A confirmação ao titular de que seus dados pessoais estão sendo processados está prevista no rol dos direitos do Art. 15 do RGPD e no Art. 19 da LGPD. Neste caso, é facultado ao titular solicitar informações adicionais, que incluem a finalidade do processamento, as categorias dos dados pessoais em questão, os destinatários aos quais os dados serão divulgados, a duração do armazenamento e a existência de decisões automatizadas, incluindo pesquisa de perfil, entre outros.

Outro direito no Art. 15, vinculado ao acesso, é que o titular seja informado de salvaguardas aplicáveis quando seus dados são transferidos para outros países. No entanto,

[90] UNIÃO EUROPEIA, RGPD: Artigo 15 "1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações"

quando se fala de DLTs, é possível que os controladores simplesmente desconheçam o conteúdo dos blocos, que é o esperado quando esse conteúdo é criptografado ou se a única informação disponível é um *hash* . WACHTER *et al* (2017)[91] ressalva que

> O requisito de notificação antes do processamento se aplica apenas aos deveres de notificação. Em contrapartida, o direito de acesso pode ser invocado a qualquer momento pelo titular dos dados, abrindo a possibilidade de fornecer informações disponíveis após a tomada de uma decisão (ou seja, os motivos de uma decisão específica). No entanto, os pesquisadores argumentaram que as informações fornecidas por meio de obrigações de notificação e o direito de acesso são amplamente idênticas, o que significa que o direito de acesso é igualmente limitado em termos do escopo de "informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas" As informações podem, portanto, ser fornecidas com ferramentas idênticas (por exemplo, ícones, declarações de privacidade) ou modelos genéricos usados para notificação e em resposta a solicitações de acesso.

Quando uma solicitação de acesso é feita por um titular de dados, o responsável pelo tratamento deve procurar todos os seus registros (eletrônicos e em papel) para fornecer informações relacionadas ao titular dos dados. Assim, quando um controlador de dados conta com o DLT para processar dados pessoais isoladamente ou em conjunto com outros meios, deve indagar se esse banco de dados contém informações sobre o titular dos dados. De maneira geral, não há obstáculos de princípios pelos quais o Artigo 15 do RGPD não possa er implementado em relação às *blockchains*. Todavia, isso pressupõe a existência de mecanismos adequados de governança que permitam uma comunicação eficaz e gerenciamento de dados.

Os pedidos de acesso podem ser tratados pelos dados sujeitos ao responsável pelo tratamento ou, nos termos do Art. 26 do RGPD a qualquer um dos controladores conjuntos.

No entanto, ressalte-se que em algumas das entidades aptas a se qualificar como controladoras (conjuntas) sob o RGPD podem simplesmente ser incapazes de acessar dados inseridos na corrente. Em termos concretos, *a priori*, os nós têm acesso apenas ao conteúdo criptografado, seu *hash* e informações de data e local de inserção no bloco. Consequentemente,

---

[91] WACHTER, S., MITTELSTADT, B., RUSSELL, C**, Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR**, Harvard Journal of Law & Technology, vol. 31, number 2, 2018, p. 842 a 861, disponível em <https://bit.ly/2IlDZJ1>, acesso em 11/09/2019. Da p. 876: "The requirement for notification prior to processing applies only to the notification duties. 146 In contrast, the right of access147 can be invoked at any time by the data subject, opening up the possibility of providing information available after a decision has been made (i.e., the reasons for a specific decision). However, scholars have argued that the information supplied via notification duties and the right of access is largely identical, meaning the right of access is similarly limited in terms of the scope of "meaningful information about the logic involved as well as the significance and the envisaged consequences." Information can thus largely be provided with identical tools (e.g., generic icons, privacy statements) or generic templates used for both notification and in response to access requests."

esses atores podem não conseguir determinar se uma DLT realmente contém dados pessoais relacionados ao titular que tenta exercer seu direito de acesso. De forma semelhante, o responsável pelo tratamento provavelmente terá dificuldade em fornecer cópias dos dados pessoais em processamento ao seu titular, conforme reza o Art. 15(3) do RGPD.

Como corolário, qualquer ator que decida utilizar tecnologias baseadas em *blockchain* para processar dados pessoais deve garantir a existência de mecanismos de governança apropriados que permitam o efetivo exercício do Direito de Acesso (FINCK, 2019, p. 72). Novamente, o armazenamento de dados pessoais e transacionais fora da corrente é uma alternativa para solucionar esta questão.

8.4. O DIREITO AO ESQUECIMENTO

O Direito ao Esquecimento talvez seja o aspecto de mais fácil compreensão da população em geral, em função de suas implicações concretos no que toca à reputação individual.

Por "Direito ao Esquecimento", entende-se o direito que uma pessoa ou entidade tem de se opor à lembrança de fatos verídicos que são jurídico ou moralmente reprováveis, que, de acordo com DINIZ(2017)[92], foram (...)*outrora praticados por ela, que perderam, pelo decurso do tempo, a atualidade e que só devem ficar na sua memória por constituir a sua própria história, evitando que sua republicação seja um obstáculo à sua vida presente.*

Trata-se, desta maneira, da faculdade que o titular de um dado ou fato pessoal tem para vê-lo apagado, suprimido ou bloqueado, especialmente pelo seu decurso no tempo que, de alguma maneira, ferem seus direitos fundamentais (CHEHAB, 2015)[93].

Segundo TRIGUEIRO (2016, p.87)[94]:

> (...) observa-se que acerca do direito ao esquecimento destacam-se os seguintes modos de exercício: a prerrogativa de inibir a divulgação de fatos mal avaliados, em cujo o titular teve participação (inclusive passivamente ou na condição de vítima); o poder de exigir a observância de uma visão prospectiva a respeito de sua identidade pessoal; e ainda a faculdade de determinar a retificação e o apagamento de informações a seu respeito constantes dos assentos de instituições públicas e privadas. O direito ao

[92] DINIZ, M. H., **Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido.** Revista Brasileira de Direito, Passo Fundo, v. 13, n. 2, p. 7-25, 2017.
[93] CHEHAB, G., **O direito ao esquecimento na sociedade da informação**. Revista dos Tribunais, v. 104, n. 952, p. 85-119, fev. 2015.
[94] TRIGUEIRO, F. V. M., **Direito ao esquecimento: dimensão da intimidade e identidade pessoal**. Revista de Direito Constitucional e Internacional, vol. 98, ano 24, p. 83- 107, nov/dez, 2016.

> esquecimento pode ser invocado ainda por terceiros afetados por fatos ou realidades ligados a parentes e pessoas próximos.

A questão foi amplamente discutida durante o projeto do Marco Civil da Internet[95] (MCI - Lei nº 12.965/2014), contida nos seus Arts. 2º e 3º (BELLI, 2018)[96], e continua a ser controversa nos tribunais[97], dado que tecnologias de *Big Data*, buscadores e afins, tal como se encontram atualmente, representam uma afronta a este direito. Na LGPD[98], o assunto é tratado de maneira direta no Art. 16: uma vez que cesse a utilização dos dados para a finalidade devida, eles devem ser destruídos. Porém, as exceções e limitações descritas nesse artigo mostram que o Direito ao Esquecimento não é absoluto: há situações em que se admite manter os dados por um período muito mais extenso do que sua finalidade original.

O Art. 17 do RGPD fala do "Direito ao apagamento dos dados", que encontra correspondência no inciso VI do Art. 18 da LGPD[99], em que o titular dos dados tem garantia formal que seus dados pessoais sejam apagados sem demora injustificada.

---

[95] BRASIL, Lei nº 12.965/2014: "Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
I - o reconhecimento da escala mundial da rede;
II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
III - a pluralidade e a diversidade;
IV - a abertura e a colaboração;
V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VI - a finalidade social da rede.
Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
IV - preservação e garantia da neutralidade de rede;
V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
VII - preservação da natureza participativa da rede;
VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte."

[96] BELLI, L., **STJ consagra direito ao esquecimento na Internet: o que isso significa?**, Portal Jota, 20/05/2018, disponível em <https://bit.ly/2Jp2Eik>, acesso 11/09/2019.

[97] Vide julgados como Recurso Especial nº 1.334.097 e Recurso Extraordinário nº 1.010.606

[98] BRASIL, LGPD, "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

[99] *Ibdem*, "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;"

Quando receber um pedido de apagamento de dados, o responsável pelo tratamento de dados deve adotar medidas razoáveis para fazê-lo "tendo em consideração a tecnologia disponível e os custos da sua aplicação", conforme apregoa o item 2 do Art. 17 do RGPD. Em seguida, o responsável deve informar a ação tomada ao solicitante, bem como se existem cópias ou reproduções daqueles dados.

Ocorre que a dificuldade de mudar um dado inserido num *blockchain* é uma de suas características mais relevantes: por definição, um dos motivadores para se ter uma rede descentralizada é resistir às tentativas de censura pela exclusão ou alteração de dados.

No estágio de uso que as DLTs se encontram atualmente, não é viável a aplicação direta do Direito ao Esquecimento. No que diz respeito aos dados transacionais, é possível tentar utilizar algumas soluções, como manter um banco de dados criptografado, porém alterável, que aponte para dados contidos num *blockchain* sem alterá-lo. Em contraste, a conformidade com os regimes de proteção de dados é certamente mais onerosa quando se trata de chaves públicas armazenadas em registros de *blockchains*.

FINCK(2018, p. 30) questiona especificamente o termo 'tecnologia disponível', entendendo que este termo poderia levar a uma interpretação mais larga do RGPD, em que as limitações técnicas impostas pelas DLTs obrigariam ao apagamento apenas parcial de dados:

> Diferentemente da eliminação definitiva, os dados criptografados ainda existiriam na cadeia, mas só poderiam ser acessados pelo titular dos dados (através de seu controle exclusivo da chave privada) ou simplesmente não mais ser acessados. A remoção pode ser usada para excluir transações obsoletas em blocos mais antigos que não são mais necessários para a continuação da cadeia, mas a ideia permanece controversa.

Uma opção para garantir o exercício do Direito ao Esquecimento em DLTs está na utilização de algoritmos de *chameleon hashes*[100], que são funções que utilizam uma chave secreta *(trapdoor)* para alterar o registro sem alterar o *hash*. Isso permite que algum moderador, em situações bastante restritas e com total transparência e responsabilidade, reescreva o conteúdo dos blocos sem alterar seu *hash* identificador. Contudo, esta abordagem é controversa.

Um problema que deve ser considerado imediatamente é o da perda da chave de bloqueio, que torna o *blochain* imutável. Além disso, a existência do moderador reintroduziria a necessidade de terceiros confiáveis, o que pode ser inaceitável para diversas pessoas, especialmente ao se tratar de DLTs abertas. O uso de *Chameleon hashes* também não elimina

[100]ATENIESE, G., MEDEIROS, B., **Identity-Based Chameleon Hash and Applications**, In: Juels A. (eds) Financial Cryptography. Lecture Notes in Computer Science, vol 3110. Ed. Springer, 2004, disponível em <https://bit.ly/32WfTN7>, acesso em 11/09/2019.

as cópias mais antigas da corrente que teve informações editadas, pois mineradores têm discricionariedade quanto aceitar ou não as alterações.

Na tentativa de alterar dados já inseridos num *blockchain*, *hard forks* seriam uma alternativa em casos excepcionais[101]. FINCK(2018, p. 30), porém, explica que mesmo uma solução tão drástica não garante a conformidade com o RGPD. Sob o ponto de vista meramente técnico, *hard forks* só fazem sentido para alterar dados no bloco minerado mais recente, pois todos os blocos subsequentes são invalidados, obrigando que todas as transações armazenadas nesses blocos sejam reprocessadas. Independentemente dos protocolos de consenso aplicados, esta é uma opção cara e que demanda muito tempo (assumindo igual ao tempo decorrido desde a mineração do bloco e assumindo igual poder de mineração).

Novamente, assim como em diversos outros termos, há alguma imprecisão no significado de "apagamento" no RGPD, abrindo a porta para outras interpretações além da exclusão absoluta.

Nessa imprecisão, vale a pena notar que certos países que já têm suas leis nacionais de implementação adotam uma versão mais suave do direito de ser esquecido. Na Alemanha[102], a lei afirma claramente que é possível que dados não sejam excluídos quando o modo específico de armazenamento não o permita:

> (1) Se a exclusão no caso de processamento de dados não automatizado não for ou apenas for possível com custos desproporcionalmente altos devido à natureza especial do armazenamento e se o interesse do usuário na exclusão for considerado baixo, o direito do titular dos dados existe Dever da pessoa responsável pelo apagamento dos dados pessoais a que se refere o artigo 17.o, n.o 1, do Regulamento (UE) 2016/679, de complementar as exceções referidas no artigo 17.o, n.o 3, do Regulamento (UE) 2016/679. Nesse caso, a supressão é substituída pela limitação do processamento, em conformidade com o artigo 18.o do Regulamento (UE) 2016/679. As frases 1 e 2 não se aplicam se os dados pessoais tiverem sido processados ilegalmente.

---

[101] Um caso famoso é o que ocorreu com o hack do DAO (*Distributed Autonomous Organization*) no Ethereum. Ethereum é uma plataforma descentralizada baseada no *blockchain* do Bitcoin, cujo diferencial é a possibilidade de programação de *smart contracts*. Em 2016, sofreu um ataque ("The DAO hack") que gerou um *hard fork* em seu *blockchain,* dando origem a duas correntes diferentes: uma sem alteração após o ataque, outra, com a alteraçãodos dados. Mais informações em <https://bit.ly/2K37pwa >, acesso 11/09/2019.

[102]ALEMANHA, **Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680**, 2016, disponível em <https://bit.ly/2lNRBV9>, acesso em 13/09/2019. Art. 35(1): "(1)Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Spei- cherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezoge- ner Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden".

Conforme o excerto acima, em tais circunstâncias, é tolerada uma solução alternativa de não excluir, mas apenas limitar o processamento de dados. Ainda não se sabe como isso se aplicará a DLTs. Por exemplo, desde que uma chave pública esteja na corrente, ela sempre será 'processada', pois sempre fará parte do *hash* qual novos blocos, ainda que indiretamente. É uma das características desse tipo de tecnologia. A aplicabilidade do Direito ao Esquecimento, portanto, carece de um delineamento melhor.

9. CONCLUSÃO

Com base na literatura analisada neste trabalho, é possível dizer que a pergunta “por que o assunto “Blockchain” teria relevância para o Direito?” foi respondida. Tratando as tecnologias em geral como sistemas peritos, sua subsunção ao Direito ocorre de maneira natural, ao mesmo tempo em que o Direito se transforma a partir dos instrumentos existentes.

Teleologicamente, as sociedades buscam a confiança e segurança por meio de suas instituições. DLTs são ferramentas potencialmente capazes de oferecer ambas, a depender de como aplicadas. Retomando o pensamento de Kevin Werbach, há oportunidades de negócio a serem aproveitadas. Primavera De Filippi vai além e prevê, com certo ufanismo, uma revolução social pela tecnologia. Em contraste, Michèle Finck faz uma análise sobre limitações bastante concretas na utilização de DLTs perante a legislação vigente.

De fato, DLTs devolvem aos usuários de sistemas de informação distribuídos a noção de escassez e de exclusividade. Tal noção tem especial relevância nas situações em que a singularidade é importante, como no caso do controle de identidade ou de propriedade, temas igualmente pertinentes para o mundo jurídico e da tecnologia.

Ainda não há consenso construído sobre regular ou não essas tecnologias, mas há tentativas ao redor do mundo de fazê-lo, particularmente no que tange às criptomoedas. Gradativamente, outras aplicações para essas tecnologias são experimentadas, o que tem levado ao surgimento de “evangelistas” tecnológicos, os quais apregoam a resolução de todos os problemas pela utilização desta ou daquela tecnologia.

Essa falta de consenso denota, por outro lado, que o Estado é limitado em sua capacidade de atuação, pois os sistemas não reconhecem limites de jurisdição ou autoridade institucional central. Ademais, há direitos consagrados que são diretamente afetados pelo uso massivo dessas tecnologias, com destaque para as questões de privacidade e as liberdades individuais.

À medida que o uso de DLTs se populariza, percebe-se um movimento de inovação intenso no Direito e nos negócios, mas ainda sem previsão de acomodação social no curto prazo. Aliado a isso, os agentes do Estado e os legisladores ao redor do mundo procuram se apropriar dos conceitos e identificar seus limites de regulação. Contudo, há um claro questionamento do protagonismo do Estado, enfraquecendo qualquer pretensão ser o definidor do que é válido e justo.

No atual estágio de desenvolvimento, não há autoridade capaz de regular o uso da tecnologia, nem um *locus* de arbitragem universal, nem definições suficientemente claras de condutas criminosas. Desta maneira, a relação entre DLTs e o Direito reaviva a própria discussão dos limites da inovação tecnológica, porém, em escala mundial.

REFERÊNCIAS

ALEXY, R., C**onceito e Validade do Direito**, tradução de G. B. O, Mendes, 1ª ed., São Paulo, Editora Martins Fontes, 2011, p. 101 a 112.

ARAÚJO, V. S. **O princípio da proteção da confiança: uma nova forma de tutela do cidadão diante do Estado**, Ed. Impetus, 2009.

ATENIESE, G., MEDEIROS, B.**, Identity-Based Chameleon Hash and Applications**, In: Juels A. (eds) Financial Cryptography. Lecture Notes in Computer Science, vol 3110. Ed. Springer, 2004, disponível em <https://bit.ly/36ZmLvG>, acesso em 11/09/2019.

ÁVILA, H. **Segurança jurídica: entre permanência, mudança e realização no direito tributário**. 2. ed. São Paulo: Malheiros, 2012.

BANAKAR, R., **Normativity in Legal Sociology**, Ed. Springer, 2015.

BANTON, M., **The Social Anthropology Of Complex Societies**. New York: Frederick A. Praeger, 1966, p. 1-18

BELLI, L., **STJ consagra direito ao esquecimento na Internet: o que isso significa?**, Portal Jota, 20/05/2018, disponível em <https://bit.ly/2Jp2Eik>, acesso em 11/09/2019.

BOBBIO, N., **Teoria da Norma Jurídica,** 1ª ed., Bauru, Edipro, 2001, p. 45- 62.

BOURDIEU, P., **Sobre o Estado: Cursos no Collège de France (1989-92)**, Ed. Companhia das Letras, 2014.

BRAGA, B. C. M., **Os princípios da segurança jurídica, confiança legítima e boa-fé: breves notas distintivas**, 2014, disponível em <https://bit.ly/2Ioewwu>, acesso em 15/05/2018.

BRASIL, **Constituição da República Federativa do Brasil**, 5 de outubro de 1988.

_____, **Código de Processo Civil,** Lei nº 13.105, de 16 de março de 2015.

_____, **Marco Civil da Internet**, Lei nº 12.965, de 4 de abril de 2014.

_____, **Lei Geral de Proteção de Dados (LGPD)**, Lei nº 13.709 de 14 de agosto 2018

_____, Supremo Tribunal Federal, **Súmula Vinculante 1**, publicada no DOU de 06/06/2007.

_____, Supremo Tribunal Federal, **Súmula Vinculante 9**, publicada no DOU de 20/06/2008.

_____, Supremo Tribunal Federal, **Súmula Vinculante 35**, publicada no DOU de 20/10/2007.

_____, Supremo Tribunal Federal, Rcl 10.707 AgR, voto do rel. min. Celso de Mello, j. 28-5-2014, P, DJE de 30/10/2014

CASTELLS, M., **La Era de la información: economía, sociedad y cultura**. México: Siglo Veintiuno Editores, 1999, p. 32, disponível em <https://bit.ly/30dApHQ>, acesso em 20/09/2019.

CASTILLO BLANCO, F. A., **La protección de confianza en el derecho administrativo**, Marcial Pons Ediciones Jurídicas y Sociales, 1998.

CHEHAB, G., **O direito ao esquecimento na sociedade da informação**. Revista dos Tribunais, v. 104, n. 952, p. 85-119, fev. 2015.

CLAES, E., KROLIKOWSKI, M , **Facing the Limits of the Law,** Springer Science & Business, 2009.

DE FILIPPI, P., HASSAN, S., **Blockchain Technology as a Regulatory Technology From Code is Law to Law is Code**, First Monday, Volume 21, Number 12 - 5 December 2016 , disponível em <https://bit.ly/2qKi34l>, acesso em 11/09/2019.

DE FILIPPI, P., WRIGHT, A., **Decentralized Blockchain Technology and the Rise of Lex Cryptographia**, 2015, disponível em <https://bit.ly/1JXbOxe>, acesso em 14/10/2019:

DEUTSCHE WELLE, **Blockchain: Paying with bits and bytes**, 10/05/2019, disponível em <https://bit.ly/2mdu2VQ>, acesso em 23/09/2019.

DI PIETRO, M. S. Z., **O STJ e o princípio da segurança jurídica**, Portal Migalhas, 15/05/2019, disponível em <https://bit.ly/2k5zKII>, acessado em 11/09/2019.

DIDIER JR., F., **Curso de direito processual civil: introdução ao direito processual civil, parte geral e processo de conhecimento**, vol. I, 17a ed., Salvador: Ed. Jus Podivm, 2015.

DINIZ, M. H., **Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido. Revista Brasileira de Direito**, Passo Fundo, v. 13, n. 2, p. 7-25, 2017.

FAIRFIELD, J., **Smart contracts, Bitcoin bots, and consumer protection**. Wash. & Lee L. Rev. Online 71, 2104, 35-299, disponível em <https://bit.ly/2njxBue>, acesso em 11/09/2019.

FERREIRA, P. C. A, **O Princípio da Confiança: Proteção e Tópica Jurisprudencial dos Contratos de Saúde Suplementa**r, Revista de Direito Civil Contemporâneo | vol. 2/2015 | p. 83 - 107 | Jan - Mar / 2015, disponível em <https://bit.ly/2kvPhBU>, acesso em 11/09/2019.

FINCK, M., **Blockchains and Data Protection in the European Union**, European Data Protection Law Review, Volume 4, Issue 1, 2018.

_____., **Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?**, European Parliamentary Research Service, julho, 2019, disponível em <https://bit.ly/2lxNLPE>, acesso em 09/09/2019.

GARNER, B. A., **A dictionary of modern legal usage**. Oxford University Press, USA, 2001.

GIDDENS, A., **As Consequências da Modernidade**. São Paulo: Editora Unesp, 1991, disponível em <https://bit.ly/1CQiUQb>, acesso em 07/09/2019.

GOLDMAN SACHS, **Blockchain - The new technology of trust**, [S.l: s.n.], disponível em <https://bit.ly/2Lpctck>, acesso em 23/09/2019.

IDC GROUP, **Worldwide Blockchain Spending Forecast to Reach $2.9 Billion in 2019, According to New IDC Spending Guide**, Portal do IDC, 04/03/2019, disponível em <https://bit.ly/2F5c8vy>, acesso em 23/09/2019

KELSEN, H., **Teoria pura do Direito**, 6ª ed, Ed. Martins Fontes, São Paulo,1998

KNIJNIK, D., **O princípio da segurança jurídica no direito administrativo e constitucional.** Revista do TCE-RS, v. 13, p. 148

KUMAR, V, CHERJELA, B, MADRIA, S, MOHANIA, M, **A Survey of Trust and Trust Management in Cloud Computing**, *in* Managing trust in the Cyberspace, CRC Press, 2014, disponível em <https://bit.ly/2CIvLax >, acesso em 12/11/2019.

LESSIG, L., **Code and Other Laws of Cyberspace**, Ed. Basic Books, 1999.

LÉVY-BRUHL, H., **Sociologia do Direito**, Ed. Martins Pena, 1997.

LOUREIRO, L. G., **Registros Públicos -Teoria e Pratica**, 8ª ed., Editora Jus Podivm, 2017.

LUHMANN, N., **Introdução à teoria dos sistemas**. 3ª. ed. Petrópolis: Vozes, 2009.

MAFFINI, R., **Princípio da proteção da confiança legítima**. Enciclopédia jurídica da PUC-SP. ed. Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://bit.ly/2kBzth0>, acesso em 11/09/2019.

MAURER, H., **Direito administrativo geral**. Barueri: Manole, 2006.

MAYER, M, MARTINO, L., MAZURIER, P., TZVETKOVA, G., **How do you define Cyberspace?**, Portal Academia, 19/05/2014, disponível em <https://bit.ly/2MHjSaV>, acesso em 11/09/2019.

MÜLLER, A., **A Brief History of the BCL**, 2000, disponível em <https://bit.ly/33JBnxp >, acesso em 11/09/2019.

NOTHEISEN, B., HAWLITSCHEK, F., WHINHARDT, C., **Breaking down the Blockchain hype - towards a Blockchain market engineering aproach**. In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017

O'DWYER, R, **Limited Edition: Producing Artificial Scarcity For Digital Art On The Blockchain And Its Implications for The Cultural Industries**, 2018, dispovível em <https://bit.ly/2lx8dAt>, acesso em 24/09/2019.

PATEL, J, **Data Structure, Algorithms and Design Techniques**, 2009, <https://bit.ly/2lBATbk>, acesso em 07/09/2019.

POSCHER, R., **Ambiguity and Vagueness in Legal Interpretation**, 2011, disponível em <https://bit.ly/2myyYVC>, consultado em 24/09/2019.

REIDENBERG, J. R., Lex Informatica: The Formulation of Information Policy Rules Through Tecnology, Texas Law Review, vol. 76, n. 3, 1998, disponível em <https://bit.ly/2lOJkjB>, acesso em 12/09/2019.

TAPSCOTT, D., TAPSCOTT, A, **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**, Ed. Penguin, 2016.

TARTUCE, F., **Manual de direito civil: volume único**, 7ª ed., Ed. Método, 2017.

THE ECONOMIST, **Blockchains: The great chain of being sure about things**, 31/10/2015, disponível em <https://econ.st/2IFp6Ds>, acesso em 23/09/2019.

THE NEW YORK TIMES, **Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens**, 19/03/2018, disponível em <https://nyti.ms/2mOCACK>, acesso em 24/09/2019.

VOS, J., **Blockchain based land registry: panacea, illusion or something in between?**, ELRA,7th annual encounter, 2017, disponível em <https://bit.ly/2m2lC3w>, acesso em 11/09/2019.

WACHTER, S., MITTELSTADT, B., **A right to Reasonable Inferences: Re-thinking Data Orotection Law in the age of Big Data and AI**, Columbia Business Law Review, 2019, disponível em <https://bit.ly/2VcrRzn>, acesso em 11/09/2019.

WACHTER, S., MITTELSTADT, B., RUSSELL, C., **Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR,** Harvard Journal of Law & Technology, vol. 31, number 2, 2018, pgs. 842 a 861, disponível em <https://bit.ly/2IlDZJ1>, acesso em 11/09/2019.

WEF, **Blockchain Beyond the Hype A Practical Framework for Business Leaders**, 2018.

____, **Deep Shift Technology Tipping Points and Societal Impact, Survey Report**, 2015, disponível em <https://bit.ly/1KlN8ZR>, acesso em 05/09/2019.

____, **Blockchain Beyond the Hype A Practical Framework for Business Leaders**, 2018, tradução livre, disponível em <https://bit.ly/2HoLWL2>, consulta em 11/09/2019

WEGNER, P., REILLY, E. D., **Encyclopedia of Computer Science**. UK: John Wiley and Sons, 2003.

WERBACH, K., CORNELL, N., **Contracts Ex Machina**, Duke Law Journal, 67, 2017, disponível em <https://bit.ly/2ObVgGv>, consultado em 11/09/2019.

YAHOO FINANCE, **Blockchain Is Revolutionizing The Way We Do Business**, 20/08/2019, disponível em <https://yhoo.it/2l7I3nN>, consultado em 21/09/2019.

ZARSKY, Z. T., **Incompatible: The GDPR in the Age of Big Data**, Seton Hall Law Review Vol. 47:995, 2017, pgs. 1009 e 1010, disponível em <https://bit.ly/2DEgcS>, acesso em 15/09/2019.

ANEXO A – CRIPTOGRAFIA

"Criptografia" é um ramo da criptologia que trata do conjunto de técnicas usadas para cifrar e recuperar alguma mensagem a partir de algum método, que é utilizada desde a antiguidade. Atualmente, com os sistemas de informações digitais, refere-se a algoritmos aplicados sobre blocos ou fluxos de dados para prover confidencialidade (apenas as partes autorizadas têm acesso à informação), autenticidade (a identidade das partes) e integridade (a garantia de que não ocorreu alteração da mensagem durante seu trânsito), além de irretratabilidade (também conhecido como não-repúdio[103]: garante-se que o autor não negue sua autoria). Engloba assuntos como cifras, chaves, sistemas criptográficos, *hashes*, entre diversos outros. Em contraste, "criptoanálise" diz respeito ao conjunto de técnicas para recuperar a mensagem original de um texto criptografado, que vão de força bruta e análise estatística à exploração de falhas específicas em sistemas.

De maneira geral, STALLINGS(2005, pg. 32) [104]ensina que sistemas criptográficos são caracterizados em três dimensões independentes:

- **O tipo de operações usadas para transformar texto em claro para texto cifrado:** todos os algoritmos de criptografia são baseados em dois princípios gerais: substituição, na qual cada elemento no texto simples (bit, letra, grupo de bits ou letras) é mapeado em outro elemento e transposição, em que os elementos no texto simples são reorganizados. O requisito fundamental é que nenhuma informação seja perdida (ou seja, que todas as operações sejam reversíveis). A maioria dos sistemas, denominados sistemas de produtos, envolve vários estágios de substituições e transposições.
- **O número de chaves usadas**: se o remetente e o destinatário usarem a mesma chave, o sistema será chamado de criptografia simétrica, chave única, chave secreta ou convencional. Se o remetente e o destinatário usarem chaves diferentes, o sistema será chamado de criptografia assimétrica, de duas chaves ou de chave pública.

---

[103] NIST, **FIPS PUB 186-4 - Digital Signature Standard (DSS)**, 2013, disponível em <https://bit.ly/2IS0m90>, acessado em 11/09/20109. "A digital signature algorithm allows an entity to authenticate the integrity of signed data and the identity of the signatory. The recipient of a signed message can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time. A digital signature algorithm is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication."

[104] STALLINGS, W., **Cryptography and Network Security Principles and Practices**, 4th Ed.. Prentice Hall, 2005.

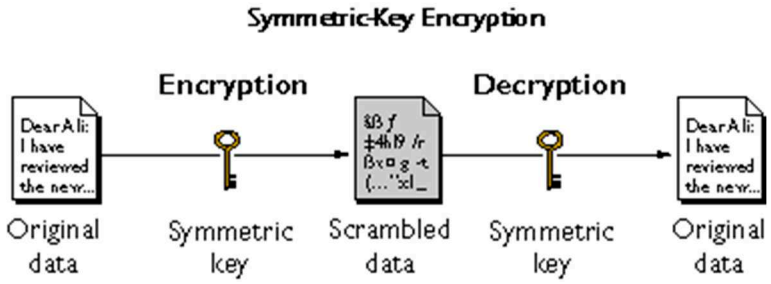
- **A maneira pela qual o texto simples é processado**: uma cifra de bloco processa a entrada de um bloco de elementos por vez, produzindo um bloco de saída para cada bloco de entrada. Uma cifra de fluxo processa os elementos de entrada continuamente, produzindo um elemento de cada vez, à medida que avança.

SISTEMAS CRIPTOGRÁFICOS SIMÉTRICOS E ASSIMÉTRICOS

Em **sistemas de criptografia de chave simétrica**, apenas uma chave é utilizada tanto para cifrar quanto para decifrar uma mensagem. Por "chave", entenda-se um segredo (normalmente, um código) compartilhado exclusivamente entre o grupo interessado (o vazamento da chave compromete todo o sistema). É passível de implementação por hardware ou software, o que garante bom desempenho na execução das operações, embora cada um dos participantes tenha de ter uma cópia do segredo.

Com essa situação representa um fator de risco, uma das soluções é a troca constante das chaves, com mecanismos de distribuição baseados em chaves assimétricas – essas, mais lentas, são utilizadas apenas para a troca, deixando a encriptação para chaves simétricas compartilhadas.

Figura 7: Criptografia Simétrica



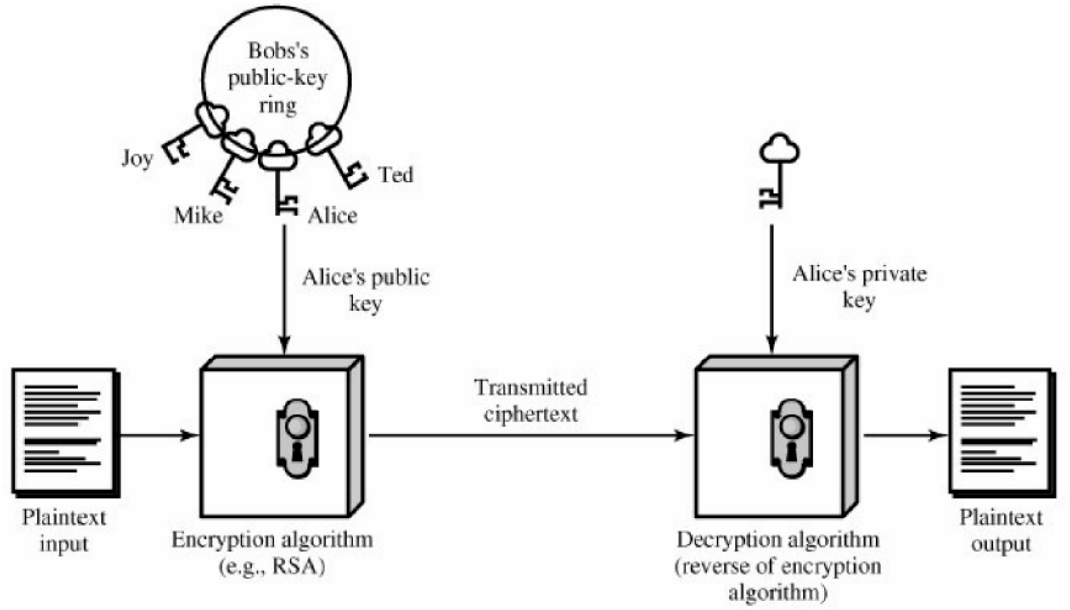
Fonte: IBM, disponível em <https://ibm.co/32E5IvG>, 11/09/2019

Sistemas de **criptografia de chave assimétrica** ou de chave pública são métodos que utilizam duas chaves: uma chave pública e uma chave privada. Esse tipo de sistema foi desenvolvido no final da década de 1970 a partir do artigo de Bailey Whitfield Diffie e de Martin Hellman (*New Directions in Cryptography*).

A chave pública é aberta e acessível a qualquer interessado. Em contraste, a chave privada é de conhecimento apenas de seu dono. Isso permite que sejam criadas chaves

públicas, as quais poderão ser mantidas em repositórios de certificação, que atuarão como terceiros de confiança. Uma mensagem criptografada com uma chave pública é decifrada apenas chave privada correspondente e vice-versa: isso dá confidencialidade à mensagem uma mensagem até seu destino, sendo também base para o funcionamento das assinaturas e certificados digitais.

Figura 8: Criptografia Assimétrica



Fonte: STALLINGS(2005, pg. 261)

Com as ferramentas apropriadas, é possível a qualquer pessoa criar pares de chaves públicas, como os utilizados nas carteiras eletrônicas do Bitcoin, que fazem uso do sistema de curvas elípticas. Já a emissão de certificados digitais por autoridades certificadoras pode exigir um processo de análise documental prévia e a utilização de *tokens* físicos.

RSA

O RSA (acrônimo para Rivest, Shamir e Adleman, que criaram o algoritmo em 1978) é a base do sistema criptográfico de chave pública mais utilizado na atualidade e sua base está em encontrar os fatores primos que compõem um número (STALLINGS, 2005).Para calcular as chaves:

- deve-se definir um valor numérico inteiro para cada símbolo do alfabeto usado;
- deve-se definir quais serão os números primos usados, p e q. Com eles, tem-se o produto n;
- calcula-se a função totiente de Euler, ou função fi: $\varphi(n) = (p - 1) * (q - 1)$;

- escolhe-se e, que é um número inteiro co-primo de φ(n) e menor que ele: 1 < e < φ(n) (co-primo é o mesmo que primo entre si);
- com esses dados, calcula-se d, que é conseguido com a seguinte equação: d x e = 1 / (mod φ(n)). Explicando: escolhe-se d de maneira que o resto da conta (d x e)/ φ(n) é 1.
- Com esses dados, tem-se a chave pública PU (e, n) e a chave privada PR (d, n).
- Para cifrar e decifrar o texto, usa-se o texto em claro M e o cifrado C, de maneira que $C = M^e \bmod n$ e $M = C^d \bmod n$, de maneira que um texto cifrado com a PR só pode ser decifrado com a PU e vice versa. É bom deixar claro que M é a representação numérica do caractere (ou conjunto deles) no alfabeto escolhido; por exemplo, a letra "s" poderia ser representada pelo número 20.

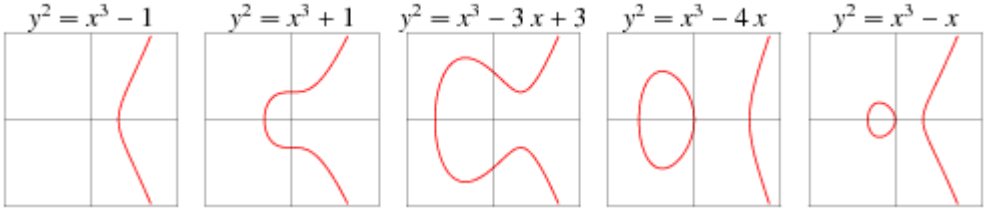
A força desse sistema está na dificuldade de fatorar números primos muito grandes.

CURVAS ELÍPTICAS

A criptografia de curvas elípticas (*Elliptic-curve cryptography* - ECC[105]) começou desenvolvida a partir de 1994, embora já se especulasse a respeito desta utilização desde a década de 1980. Esse sistema tem como base a dificuldade de se resolver Problemas do Logaritmos Discretos (PLD) em curvas elípticas[106] (*Elliptic Curve Discrete Logarithm Problem* - ECDLP). Esse tipo de criptografia utiliza chaves menores. Conforme a RFC 6090:

> O ECC é uma tecnologia de chave pública que oferece vantagens de desempenho em níveis de segurança mais altos. Ele inclui uma versão em curva elíptica do protocolo de troca de chaves Diffie-Hellman e versões em curva elíptica do algoritmo ElGamal Signature. A adoção do ECC foi mais lenta do que o previsto, talvez devido à falta de documentos normativos disponíveis gratuitamente e à incerteza sobre os direitos de propriedade intelectual.
> (...)
> Existem vários padrões que especificam ou incorporam algoritmos ECC, incluindo o Internet Key Exchange (IKE), ANSI X9.62 e IEEE P1363.

As curvas elípticas seguem a seguinte equação: $y^2 = x^3 + ax + b$:



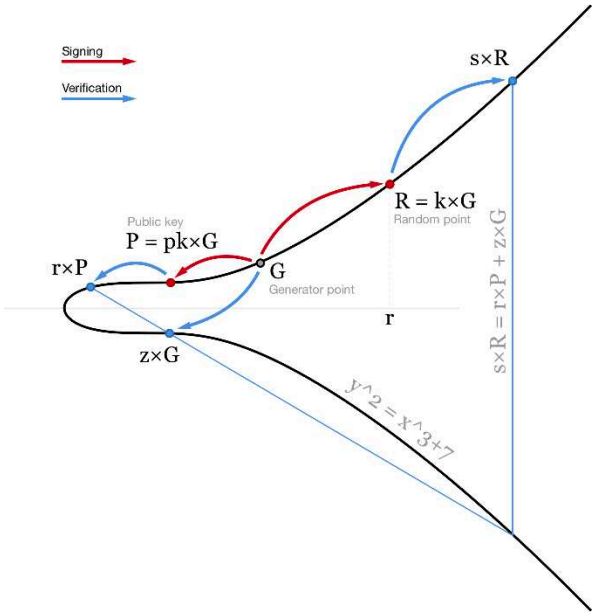
[105]IETF, **Fundamental Elliptic Curve Cryptography Algorithms**, 2011, disponível em <https://tools.ietf.org/html/rfc6090>, acesso em 11/09/2019.
[106]Para mais detalhes: <https://bit.ly/2MDKVDS> e <https://bit.ly/2pGasTS>.

Na criptografia de curvas elípticas, são realizadas operações entre pontos discretos (inteiros) num conjunto numérico finito de uma curva elíptica, que pertence a uma função matemática que apresenta simetria em relação ao eixo X.

A Figura 9 ilustra o processo de assinatura e verificação e chaves num sistema ECC:

Figura 9: Visualização do processo de assinatura digital usando curvas elípticas

(*Elliptic Curve Digital Signature Algorithm* - ECDSA)



Fonte: <*https://bit.ly/35ZlTXi*>, acesso 11/09/2019

Com uma chave privada k, gerada aleatoriamente, multiplica-se por um ponto predeterminado na curva chamado ponto gerador "G" para produzir outro ponto em algum outro lugar na curva, que é a chave pública correspondente K. No algoritmo do Bitcoin, o ponto gerador é especificado como parte do padrão secp256k[107] (há diversos outros padrões, criados por entidades como NIST, SEGG, IETF e ANSI) e é sempre o mesmo para todas as chaves:

- K = k * G
- k é a chave privada
- G é o ponto gerador
- K é a chave pública resultante, um ponto na curva

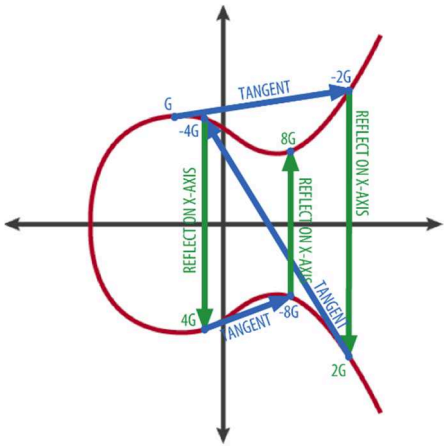
[107] MISTRY, N., **An Introduction to Bitcoin, Elliptic Curves and the Mathematics of ECDSA**. GitHub. 2015, disponível em <https://bit.ly/2MCCfNV>, acesso em 22/10/2019.

Como o ponto do gerador é sempre o mesmo para todos os usuários da rede, uma chave privada k multiplicada por G sempre resultará na mesma chave pública K. O relacionamento entre k e K é fixo, mas só pode ser calculado em uma direção, a partir de k para K. É por isso que um endereço de uma carteira (derivado de K) pode ser compartilhado sem revelar a chave privada (k).

Com uma curva elíptica sobre números reais, é possível visualizar a multiplicação de um ponto sobre um conjunto de números inteiros kG, que equivale a desenhar uma linha tangente no ponto e descobrir onde ele intercepta a curva novamente, refletindo esse ponto no eixo x.

Na Figura 10, é possível ver o processo para derivar G, 2G, 4G, como várias operações geométricas sobre uma curva elíptica:

Figura 10: Operações sobre uma curva elíptica



Fonte:<https://bit.ly/2p8drV4>, acesso 11/09/2019

ANEXO B – FUNÇÕES HASH

Funções *hash* são algoritmos que tomam uma entrada de dados de qualquer tamanho, aplicam uma série de cálculos e fornecem uma saída padronizada e, a depender do método usado, com baixíssima probabilidade de duplicação. Pelo seu processamento rápido e unicidade de resultado, são utilizados para aferir a integridade dos dados (a modificação de um único bit modifica completamente a saída), servindo para compor uma "assinatura" digital. A Tabela 1 contém um exemplo de aplicação de alguns algoritmos bastante conhecidos para a palavra "unb":

Tabela 1: Hash da palavra "unb" por diferentes algoritmos

ALGORITIMO	TAMANHO DA SAÍDA (em bytes)	SAÍDA
MD4	16	1B912FF4AADB8E447219A15FDDA2D9F1
MD5	16	A19BE82A4AF850B606D37980428AA59B
SHA-1	20	05429D90960A907F17B19F70A29D0C5E3D7F1B51
SHA-256	32	04ABD0D61FE0F7F19FD78606EED659B1DD639F3A866 913826480FE43AF66A53C
SHA-512	64	FE6A1D860960F56241536D889A469F0DAF607E2466B03 500AC4061861A7E8811FD248B499BEB0213DDD50D212 7591FCBECF8A981BC36A04B2343E91972B1C96F
Whirlpool	64	8194F7A401717D64E990F98D4805FFE5A0F11C8DA0BA 333AE29C7D3626D7E6BD02DBA13AF0C1956B1DA72B 728A00FB77707CF609F6B3825051CE4A244782EF1F

Fonte: <https://www.pelock.com/products/hash-calculator>, em 20/09/2019

Na Tabela 2, os mesmos algoritmos, aplicados para "Universidade de Brasília":

Tabela 2:Hash de "Universidade de Brasília" por diferentes algoritmos

ALGORITIMO	TAMANHO DA SAÍDA (em bytes)	SAÍDA
MD4	16	0EE881978E6FD5D8D56CEE64D64EC6DE
MD5	16	78052C025B92F26B28F19003E6CD823E
SHA-1	20	DD012E22BC10EAFDA3C885A98B8C34B5C352710B

SHA-256	32	A6DEDB3A1252A346E18C6CA99B49EF9630FE391AED153CDA2CF4E364EFA82AC0
SHA-512	64	0A4103E9DE68323A57F4F02C57D5B166A0E8F81FD3E9EC4B48833E386A94602330FB37F9630FCBCAEF09708B9CA076CA0688FB2CB638A3CF312731DB3F2FBDDD
Whirlpool	64	171AF7196B3F2B5F3C0E84724F464B10107DCC2698C36E1A42D11D1D42B473269613DFE7E220892B26E4F176CD0D71E5FB7CC98E5909EB030BD979A693802B95

Fonte: <https://www.pelock.com/products/hash-calculator>, 20/09/2019

O valor de *hash* h é gerado por uma função H do formato h = H (M), onde M é uma mensagem de comprimento variável e H (M) é o valor de *hash* de comprimento fixo. Essa função tem as seguintes propriedades (STALLINGS, 2005[108], pg. 134):

1. H pode ser aplicado a um bloco de dados de qualquer tamanho.

2. H produz uma saída de comprimento fixo.

3. O H (x) é relativamente fácil de calcular para um determinado x, tornando práticas as implementações de hardware e software.

4.Para qualquer valor dado h, é computacionalmente inviável encontrar x de modo que H (x) = h. A literatura chama isso de propriedade unidirecional: é fácil gerar um código *hash* algum bloco de dados, mas é praticamente impossível gerar uma mensagem para um código *hash*.

5. Para qualquer bloco x, é computacionalmente inviável encontrar y x de modo que H (y) = H (x). Isso é chamado de fraca resistência à colisão: garante-se que não seja possível encontrar uma mensagem alternativa com o mesmo valor que uma determinada mensagem, o que evita a falsificação quando um código *hash* criptografado é usado.

6. É computacionalmente inviável encontrar qualquer par (x, y) tal que H (x) = H (y). Tal situação é chamada de forte resistência à colisão, que diz respeito à resistência a ataques tipo aniversário.

7. As três primeiras propriedades são requisitos para a aplicação prática de uma função *hash* na autenticação de mensagens.

[108] STALLINGS, W., **Cryptography and Network Security Principles and Practices**, 4th Ed.. Prentice Hall, 2005

ANEXO C – ÁRVORES DE MERKLE

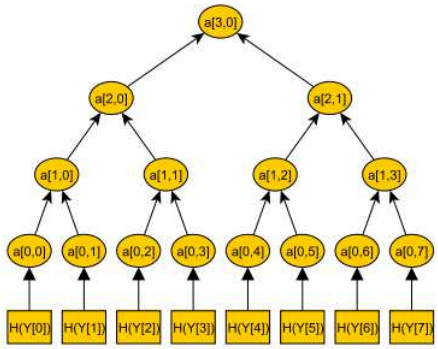
Árvores de Merkle são estruturas de dados baseadas em árvores binárias. Numa árvore binária completa, que podemos chamar de “T”, com uma altura “H”, terá 2H folhas e 2H-1 nós anteriores. Cada nó interno possui unicamente dois filhos, rotulados como "0" (esquerda) e "1" (direita). Com esta convenção de nomenclatura, as folhas são naturalmente ordenadas, indexadas de acordo com a representação binária do caminho, da raiz à folha. Visualmente, quanto maior o índice dessa folha em {0, 1, ... 2^H - 1}, mais à direita está a folha. Definimos a altitude de qualquer nó n como a altura da subárvore máxima de T da qual é a raiz. As alturas dos nós variam de 0 (folhas) a H (a raiz). Como nas folhas, os nós interiores de uma determinada altura h0 podem receber um índice em {0, 1, ... 2^{h0} - 1}(JAKOBSSON et al., 2003[109]) .

Uma árvore Merkle é uma árvore binária com uma atribuição de uma sequência para cada nó: n → P (n) ∈ {0, 1} k, de modo que os valores dos nós dos pais sejam funções *hash* dos valores dos nós filhos:

P (n-pai) = *hash* (P (n-esquerdo) || P (n-direito))

Significa que cada folha (o nó do último nível) é rotulado com o *hash* do bloco anterior, enquanto cada nó não folha é rotulado com o *hash* dos nós filhos, criando uma interdependência entre todos eles e uma forte coesão entre os nós.

Figura 11: Árvore de Merkle com 8 folhas.



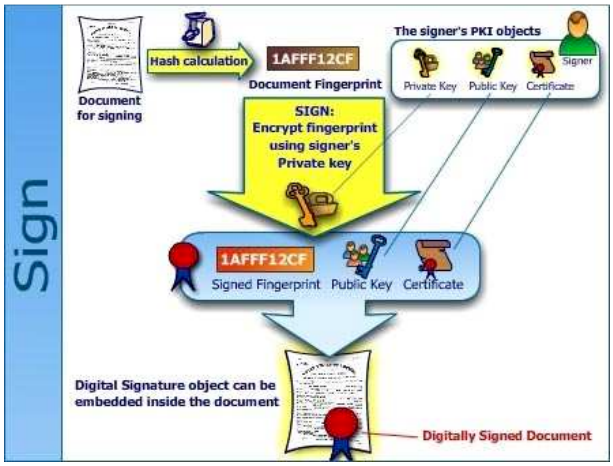
Fonte: BECKER(2008, p. 8)

[109] JAKOBSSON, M., LEIGHTON, T., MICALI, S., SZYDLO, M., **Fractal Merkle Tree Representation and Traversal**, In: Joye M. (eds) Topics in Cryptology — CT-RSA 2003. CT-RSA 2003. Lecture Notes in Computer Science, vol 2612., pgs. 314-326, Ed. Springer, 2003, disponível em <https://bit.ly/31HYGpr>, acesso em 11/09/2019.

ANEXO D – ASSINATURA DIGITAL

STALLINGS(2005) define uma assinatura digital como um *hash* de uma mensagem criptografado pela chave privada do remetente: ela garante identidade da origem e integridade da mensagem.

Figura 12: Modelo de sistema de assinatura digital baseado em criptografia de chaves públicas.

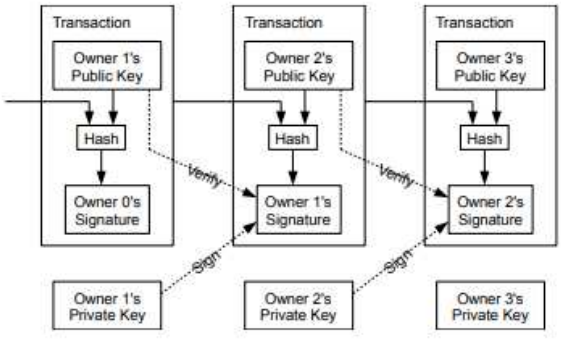


Disponível em <https://bit.ly/2Xewj1D>, acesso em 11/09/2019

Um documento assinado digitalmente nada mais é do que o *hash* do documento criptografado com a chave privada do titular do documento, que só pode ser decifrado com a chave pública respectiva, o que garante a origem da assinatura.

Na rede do Bitcoin, as assinaturas digitais são usadas a cada transação, conforme ilustra a Figura 13:

Figura 13: Transações assinadas do Bitcoin

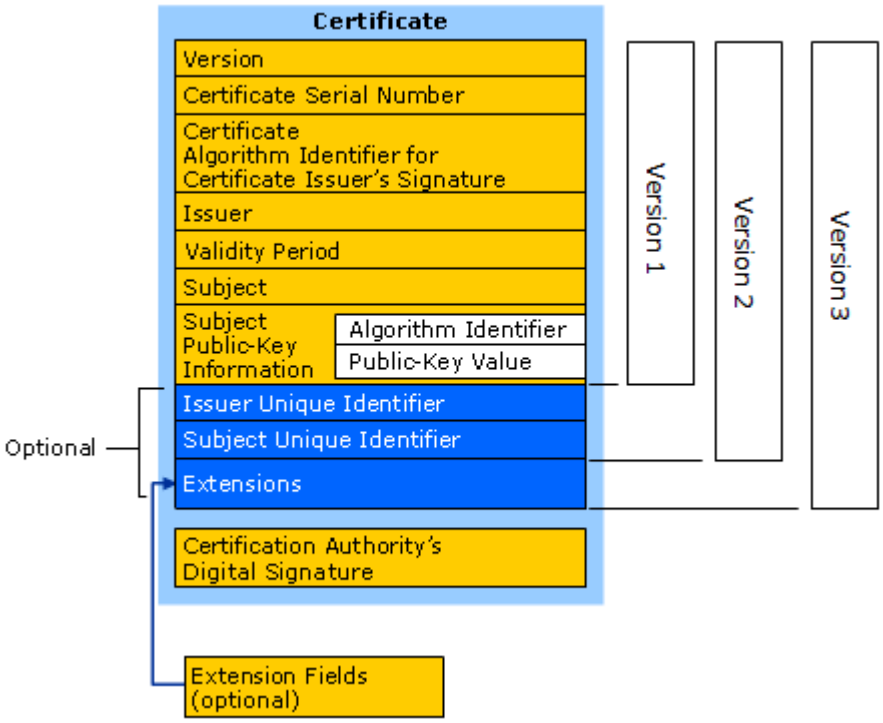


Fonte: <https://bitcoin.org/bitcoin.pdf>, acesso em 12/11/2019

ANEXO E – CERTIFICADOS DIGITAIS E INFRAESTRUTURA DE CHAVES PÚBLICAS

Certificados digitais são arquivos que contêm dados de identificação de seu titular, especialmente a sua chave pública, validade, emissor e validade, entre outros. O formato de certificado mais conhecido é o que segue o padrão ITU X.509, composto pelos seguintes campos:

Figura 14: Certificado Digital X.509: comparação de versões



Fonte:<https://bit.ly/2X7gQ32>, acesso em 11/11/2019.

Com ferramentas de software apropriadas, é possível a qualquer pessoa gerar seus próprios certificados digitais. Porém, há entidades especializadas em emitir e validar certificados digitais, chamadas de "Autoridades Certificadoras" (AC): um mediador que para garantir que o titular de determinado certificado digital realmente é quem diz ser.

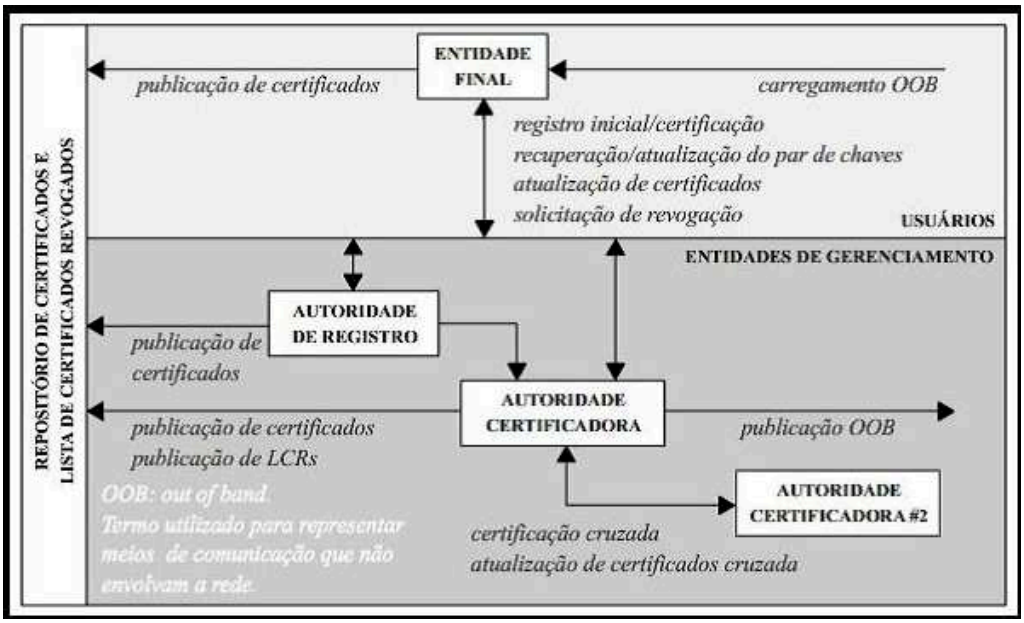
O conjunto de funções, políticas, hardware, software e procedimentos necessários para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais e gerenciar a criptografia de chave pública, dos quais as ACs fazem parte, é chamado de "Infraetrutura de Chave Pública" (ou PKI, de *Public Key Infrastructure*), cujo objetivo é facilitar a

transferência eletrônica segura de informações para uma série de atividades de rede, como comércio eletrônico.

A interface com os usuários é feita pelas Autoridades de Registro (AR), vinculadas a ACs, formando uma hierarquia que pode ter diversos níveis.

No Brasil, a ICP-BRASIL, vinculada ao Instituto Nacional de Tecnologia da Informação (ITI), regula a emissão de certificados digitais brasileiros.

Figura 15: Infraestrutura de Chaves Públicas



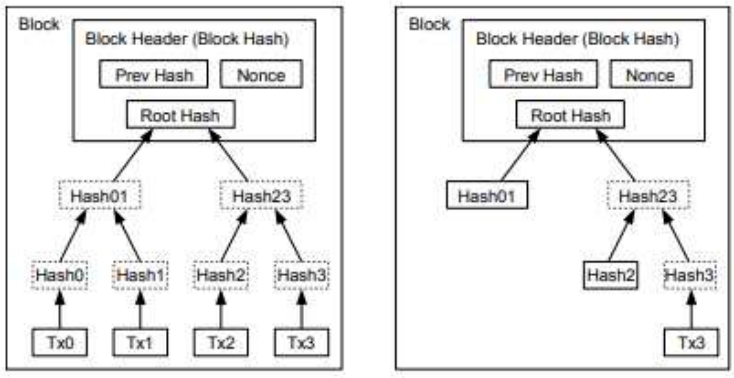
Fonte:<https://bit.ly/32CShfL>, acesso em 12/11/2019

ANEXO F – BITCOIN E BLOCKCHAIN

Bitcoin é uma um sistema de transferência e registro de valores no formato de rede P2P, em que cada participante da rede tem a possibilidade de ver todos os registros de todas as transações feitas na rede. As transações são registradas em um banco de dados composto por blocos, em que cada bloco referencia o anterior, criando uma corrente de interdependência entre os blocos.

Essa interdependência é feita por um algoritmo baseado em árvores de Merkle, que forma uma corrente de interdependência entre os blocos:

Figura 16: Transações num Blockchain



Fonte: <https://bitcoin.org/bitcoin.pdf>, acesso em 12/11/2019

Para que uma pessoa transacione com Bitcoins, é necessário que ela tenha uma identidade nessa rede, chamada de "carteira" (*wallet*). A carteira é um software, com identificador único[110] na rede, e que tem um saldo atribuído. Seu processo de criação, embora complexo, é feito de maneira rápida e o resultado pode ser guardado em diversos meios.

Uma vez que usuários da rede concordam em fazer uma transação, dados de carteira de origem, de destino e valor são difundidas na rede para compor um novo bloco de transações.

Esse bloco será validado pelo processo de mineração, que simultaneamente acrescenta um novo bloco à corrente, gera novos Bitcoins e recolhe frações de valor para

[110] O processo de geração de identificação da carteira envolve geração e concatenação de hashes de 256 bits, modificações de base e checagens. O endereço <https://bit.ly/2NK4gE1>, acessado em 12/11/2019, ilustra o processo.

compensar o processamento. A validação dos blocos é feita por meio de um algoritmo de consenso de prova de trabalho (*proof-of-work*).

No algoritmo de prova de trabalho do Bitcoin, o nó minerador constrói um bloco candidato com transações pendentes de validação. Em seguida, o minerador calcula o *hash* com algoritmo SHA-256 do cabeçalho do bloco e verifica se o valor encontrado é compatível com a dificuldade corrente na rede.

O cabeçalho do bloco consiste numa série de metadados com informações padronizadas e sequenciadas a respeito do bloco:

Figura 17: Cabeçalho de um bloco

<table>
<tr><td colspan="3">Chunk 1</td><td colspan="5">Chunk 2</td></tr>
<tr><td colspan="7">Block header</td><td rowspan="3">Padding</td></tr>
<tr><td colspan="6">Block header candidate</td><td rowspan="2">Nonce</td></tr>
<tr><td rowspan="2">Version</td><td rowspan="2">Previous hash</td><td colspan="2">Merkle root</td><td rowspan="2">Time stamp</td><td rowspan="2">Bits (difficulty)</td></tr>
<tr><td>Head</td><td>Tail</td></tr>
<tr><td>4 bytes</td><td>32 bytes</td><td>28 bytes</td><td>4 bytes</td><td>4 bytes</td><td>4 bytes</td><td>4 bytes</td><td>48 bytes</td></tr>
<tr><td colspan="3"></td><td colspan="3">Message[2]</td><td></td></tr>
</table>

Fonte:< https://bit.ly/33XSxXS>, consulta em 14/11/2019

De maneira genérica, a dificuldade é dada por uma sequência de zeros (quanto mais zeros, maior a dificuldade), de maneira que o minerador deve tentar encontrar um *hash* com valor inferior à dificuldade (com mais zeros no início do código de resultado do que a dificuldade proposta), o que só pode ser feito com o uso de força bruta: a cada tentativa, modifica-se o valor do campo "nonce" até que se encontre um resultado nos parâmetros de dificuldade.

Uma vez que a solução é encontrada, ela é propagada para a rede e os demais participantes podem fazer sua validação rapidamente.