FIAP ON

BLOCKCHAIN ADVANCED

CONCEITOS BLOCKCHAIN

FÁBIO MAÇOLI

1

LISTA DE FIGURAS

SUMÁRIO

1 CONCEITOS BLOCKCHAIN

1.1 Origem Blockchain

Figura 1.1 – Padre Luca Pacioli
Fonte: Google Imagens (2020)

A tecnologia Blockchain hoje existente teve sua origem nos idos de 1494, cuja ideia precursora era ser um livro-razão *"ledger".* Desenvolvido por um padre chamado Luca Pacioli, na sua época, consistia em promover um balanço de ativos tangíveis e intangíveis, disponibilizando de forma ordenada e detalhada várias operações de crédito e débito e a composição de um balanço final.

De acordo com o site Computeworld:

> *No livro Summa de Arithmetica, Geometria, Proportioni et Proportionalità, escrito em 1494, o frei franciscano Luca Pacioli (1445-1517) desenvolveu os primeiros estudos de matemática para serem utilizados em contabilidade. Nesses estudos, o religioso utilizou, entre outras coisas, a observação da movimentação de feiras livres com o objetivo de compreender o "Método das Partidas Dobradas", que é o sistema padrão universal de débito e crédito utilizado até hoje pelas empresas, governos e*

mercados mundiais e, não obstante, é estudado ainda hoje como matéria básica nos cursos de Administração e Negócios.
Apesar do mercado atualmente ser complexo no que diz respeito às formas de comercialização, comunicação e transação financeira, nas primeiras feiras livres já se encontrava toda a gênese das transações comerciais e financeiras, que, por incrível que pareça, ainda utilizamos em pleno século 21.

1.2 Um pouco de história

Com o surgimento da Internet, um dos pontos que apresentaram deficiência é justamente a questão relacionada à implementação de segurança. Problema este que se agravou com a quantidade de transações que emergiram do uso da Rede Mundial de Computadores, pois aos poucos ela foi se tornando uma grande ferramenta para comprar e fazer transações.

Na tentativa de mitigar tal questão, em 1971 foi criado por Horst Feisel (IBM) um algoritmo de criptografia, denominado Lucifer, baseado em um elevado nível de segurança e uma chave de codificar e descodificar.

Já em 1974 um grupo de cientistas da IBM adequou melhor a ferramenta Lucifer e surge o Data Encryption Standard (DES). A principal motivação do grupo foi justamente readequar a ferramenta criada e promover maiores índices de segurança para ela.

Em 1981, o DES foi adotado com o nome *Data Encryption Algorithm* (DEA) pela *American Standard Institution* com o principal objetivo de promover padronização de cifragem e procedimentos para serem utilizados em instituições financeiras. Desta forma, o DES se tornou o principal algoritmo de chave única.

DES é um sistema de codificação simétrico por blocos de 64 bits, dos quais 8 bits (um byte) servem de teste de paridade (para verificar a integridade da chave). Cada bit de paridade da chave (1 em cada 8 bits) serve para testar um dos bytes da chave por paridade ímpar, ou seja, cada bit de paridade é ajustado de forma a ter um número ímpar de '1' no byte ao qual ele pertence. Assim, a chave possui um comprimento útil de 56 bits, o que significa que só 56 bits são realmente usados no algoritmo.

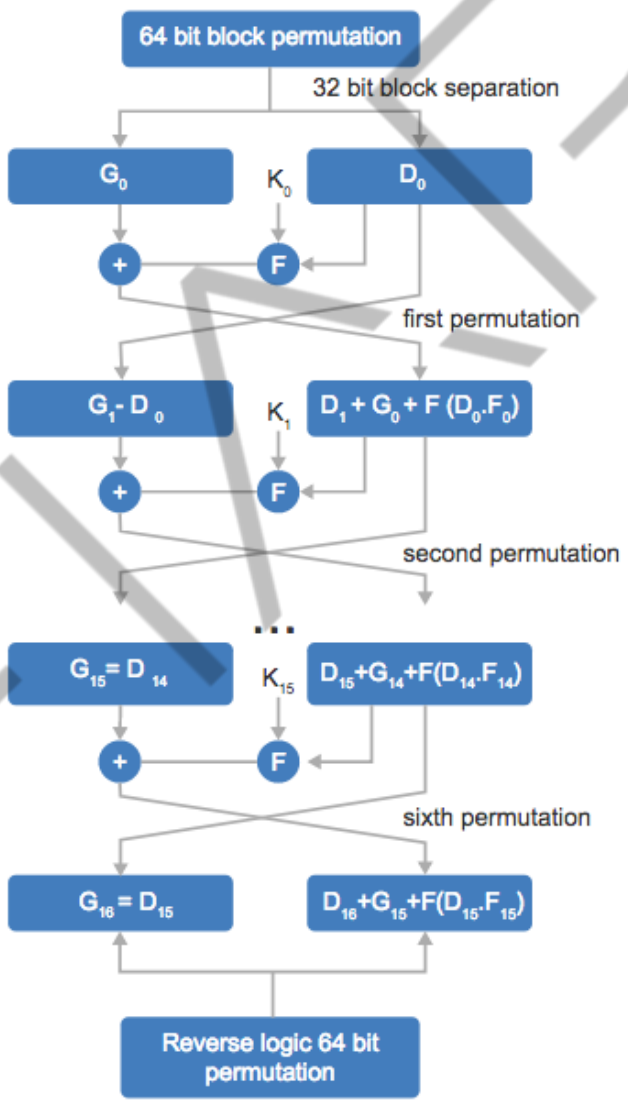

Figura 1.2 – Algoritmo do DES
Fonte: CCM (2017)

De qualquer forma, a criação do DES não foi um sucesso absoluto para evitar fraudes e vazamentos de informações. Ainda era muito inseguro promover qualquer

tipo de transação financeira pela Internet, além do sério problema de disponibilizar muitas informações pessoais do usuário do cartão.

Figura 1.3 – Segurança da Informação
Fonte: Shutterstock (2017)

Ainda na constante busca de uma solução única e eficaz para promover a segurança das transações eletrônicas, em meados de 1983, David Chaum, grande cientista e entusiasta em criptografia, fundou a DigiCash, uma empresa de moeda eletrônica criptografada.

Seu produto foi chamado de E-cash e seu objetivo era que os usuários obtivessem moedas digitais de um banco e não pudessem ser rastreados nem pelo banco nem por qualquer outra pessoa. Tal invenção foi precursora do movimento Cypherpunk, que teve seu início no final da década de 1980.

A ferramenta era tão perfeita e adequada para a época que até mesmo as grandes empresas de tecnologia se mostraram interessadas em adquiri-la. Chaum colaborou com vários outros estudos na seara da tecnologia, já propondo sistemas *peer-to-peer* (ponto a ponto) com criptografia e segurança.

Alguns relatos dizem que a solução era muito moderna para sua época. Desta forma, a empresa de Chaum, DigiCash, faliu em 1998. Parafraseando Chaum: *"*O DigiCash e seu sistema de tecnologia entraram no mercado antes que o comércio eletrônico fosse totalmente integrado na Internet*".*

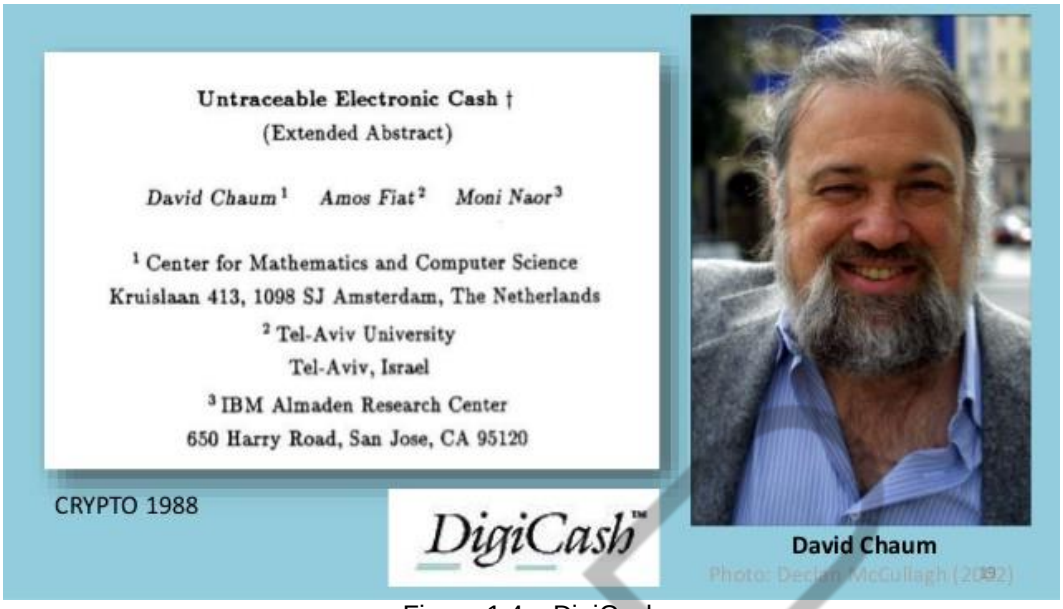

Figura 1.4 – DigiCash
Fonte: Declan McCullagh (2002)

Naquela mesma ocasião, um dos sócios da empresa DigiCash, Nick Szabo, formado em Direito e criptógrafo, promoveu a pesquisa relativa a contratos digitais e moeda digital, denominada “Contratos Digitais”. Em 2005, Szabo desenvolveu um mecanismo inovador para tratamento de uma moeda digital que recebeu o nome de bit gold. Algumas bibliografias se referem à bit gol dela como a precursora do Bitcoin.

De acordo com Tapscott (2016):

> *Nick Szabo escreveu um pequeno artigo intitulado “O protocolo de Deus”, uma variação da frase do ganhador do prêmio Nobel, Leon Lederman, com “A partícula de Deus”, referindo-se à importância do Bóson de Higgs para a Física moderna. Em seu artigo, Szabo se concentrou na criação de um protocolo de tecnologia “todo-poderoso” que designou “Deus” a terceira parte da confiança no meio de todas as transações.*
>
> *Todas as partes iriam enviar suas entradas a Deus, que, de maneira confiável, determinaria e retornaria os resultados. Deus, sendo a última palavra em discrição confessional, faria com que nenhuma das partes soubesse algo mais sobre as entradas de outros envolvidos, além de suas próprias entradas e saídas. Seu mote era contundente: fazer negócios na Internet exige um salto de fé. Porque a infraestrutura não tem toda a segurança necessária, muitas vezes, há pouca*

escolha, além de se tratar os intermediários como divindade.

Em 2008, foi lançada a moeda virtual Bitcoin, que se utiliza da plataforma Blockchain para suas transações. O lançamento da moeda foi feito por Nakamoto Satoshi, um pseudônimo, pois até os dias de hoje não se sabe precisamente quem foi o criador da moeda virtual Bitcoin. Não é sabido se se trata de uma pessoa somente ou uma equipe de cientistas que desenvolveu a tecnologia.

1.3 Motivações Blockchain

Os últimos 40 anos foram de profundos avanços tecnológicos e de inúmeras mudanças culturais nas relações humanas. A Internet passou por uma série de transformações e tecnologias que se agregaram ao princípio da comunicação de dados universal. Nos últimos anos, surgiram os grandes Datacenters, Big Data, IoT (Internet of Things*),* Cloud Computing e IPV6. E com tudo isso uma série de transformações ocorreram nas formas de relacionamento financeiras, contratuais e econômicas.

Também nos últimos anos surgiram o Uber, o Airbnb, Netflix, WhatsApp, Amazon, Spotify e outros aplicativos e apps que estão, de certa maneira, revolucionando as formas de prestação de serviço e até mesmo de relacionamento entre as pessoas. Mas toda essa revolução tecnológica ainda possui dois itens que dificultam sua plena aceitação e confiança.

Estes dois itens são a necessidade de um intermediário para todas as transações, seja um portal, uma instituição bancária, uma empresa etc., e o grande problema relacionado à segurança. Mesmo com todo o avanço tecnológico, ainda existe uma lacuna muito grande a ser tratada e saneada, que é justamente conseguir promover a segurança e integridade das transações e pagamentos efetuados na Web.

Figura 1.5 – DigiCash
Fonte: Editoria de Arte Administradores.com (2017)

No decorrer da evolução humana, várias formas de promover as relações e trocas monetárias aconteceram. Houve o momento do chamado escambo (troca de mercadorias) e, posteriormente, o surgimento das moedas, o dinheiro em papel, cartas de crédito, cartões de crédito e diversas instituições bancárias. Toda esta evolução subsidiada pelo avanço tecnológico dos grandes armazenamentos, links de comunicação, Internet, mobilidade e ferramentas de segurança.

O emprego destas novas tecnologias e o grande volume de transações ocorrendo a todo segundo, em tempo real e sem fronteiras geográficas, acabam exigindo uma ferramenta que possa promover maior rapidez, segurança, interoperabilidade, auditoria, flexibilidade e individualidade. Motivo pelo qual surge o Blockchain com o propósito de atender a todas essas demandas.

Figura 1.6 – Diferentes tipos de transação
Fonte: Elaborado pelo autor (2020)

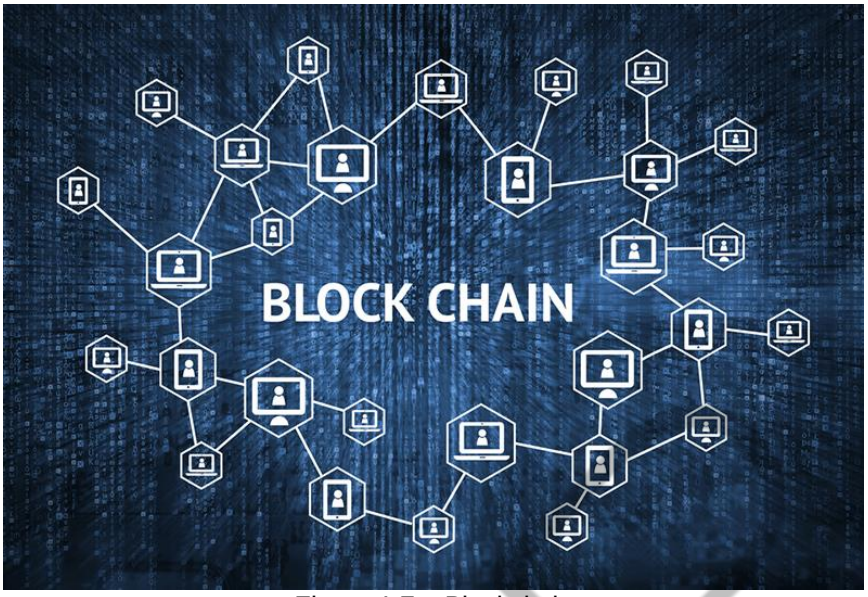

Figura 1.7 – Blockchain
Fonte: PanamericanWorld (2017)

1.4 Afinal, o que é Blockchain?

Desta forma, segundo Manav Gupta, da IBM: “Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible — a house, a car, cash, land — or intangible like intellectual property, such as patents, copyrights, or branding. Virtually anything of value can be tracked and traded on a Blockchain network, reducing risk and cutting costs for all involved”.

Blockchain é um livro-razão compartilhado e distribuído que facilita o processo de registro de transações e rastreamento de ativos em uma rede comercial. Um bem pode ser tangível – uma casa, um carro, dinheiro, terra – ou intangível – propriedade intelectual, como patentes, direitos autorais ou branding. Praticamente qualquer coisa de valor pode ser rastreada e negociada em uma rede de blocos, reduzindo riscos e também os custos para todos os envolvidos.

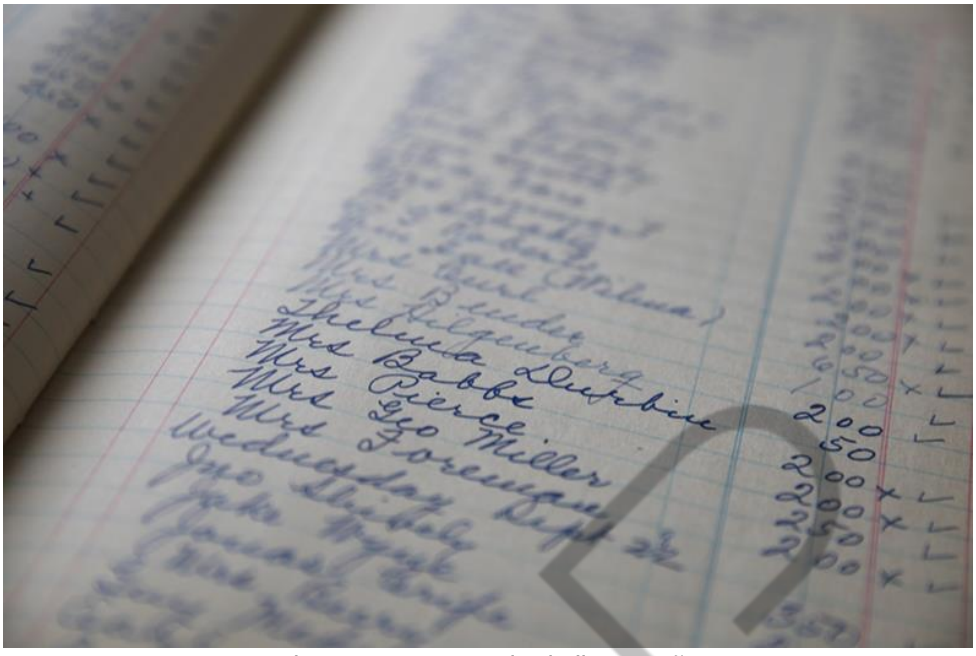

Figura 1.8 – Exemplo de livro-razão
Fonte: PanamericanWorld (2017)

Literalmente, a palavra “Blockchain” significa “cadeia de blocos” e é uma tecnologia para uma nova geração de aplicações transacionais que estabelece confiança, prestação de contas e transparência enquanto simplifica de forma eficiente os processos de negócio.

É um banco de dados distribuídos, sendo praticamente invulnerável a falhas e adulterações, e as múltiplas utilidades descolam-se da tecnologia da criptomoeda bitcoin – para a qual foi criada.

Antes do desenvolvimento da tecnologia Blockchain, os registros contábeis eram mantidos em bancos de dados centralizados e não públicos. As pessoas precisavam confiar na idoneidade do banco de dados para ter certeza de que não haveria nenhuma alteração nos registros (saldos e transações da conta).

Com o Blockchain, os dados são distribuídos entre todos os participantes, com total transparência e descentralização. Torna-se, portanto, desnecessário confiar em uma terceira pessoa para que os dados contábeis sejam registrados corretamente e não haja perigo de fraudes.

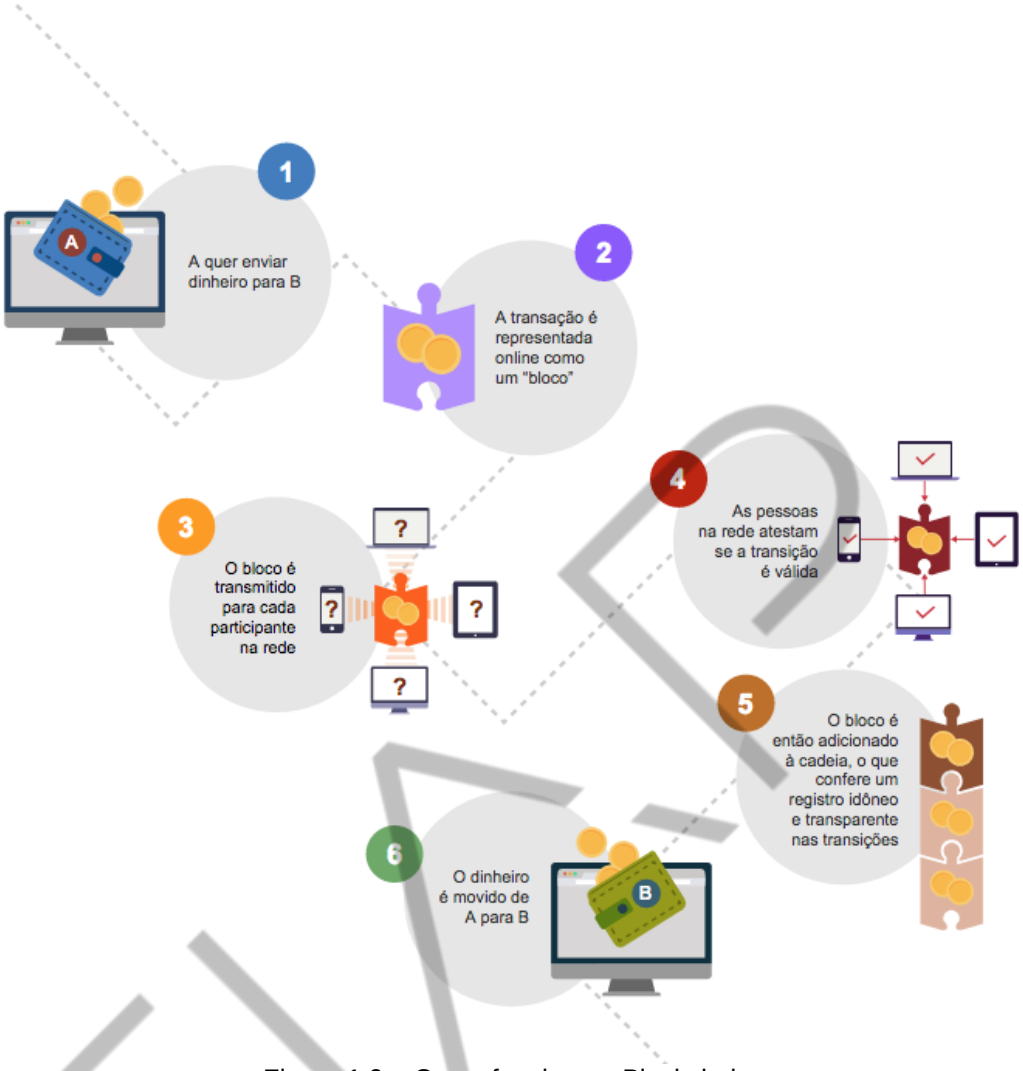

Figura 1.9 – Como funciona o Blockchain
Fonte: Blog MJV (2016)

Diante das definições acima, podemos concluir que o modelo de solução Blockchain assemelha-se a um “livro-razão”, ou seja, uma base de dados com entrada de diversos dados e transações. Todas as informações imputadas e contidas na ferramenta são compartilhadas entre vários usuários.

E o processamento desta base de dados é feito em blocos, “*de tempos em tempos”,* criando um código de verificação a cada bloco processado. Estes códigos de verificação são criados com base nos blocos processados anteriormente, fazendo com que o Blockchain seja uma solução de alta confiabilidade, pois, uma vez adulterado um bloco, isso impactará em todos os demais blocos processados.

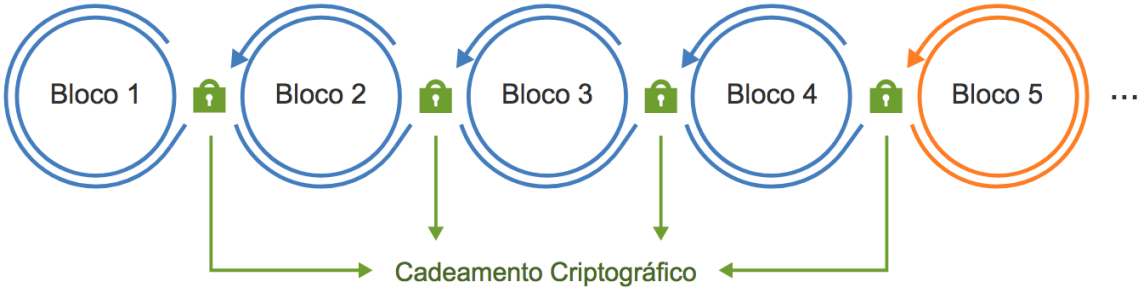

Figura 1.10 – Encadeamento criptografado
Fonte: Proof (2017)

1.4.1 Principais vantagens do Blockchain

- Total Transparência.
- Descentralização.
- Total Segurança.
- Confiança.
- Automatização.
- Flexibilidade.
- Auditável.
- Sustentável.
- Privado.
- Rastreamento.

Figura 1.11 – Confiabilidade Blockchain
Fonte: Deal (2017)

Embora o Bitcoin – assunto que será tratado com mais detalhes ao longo deste material – tenha encontrado terreno promissor e fértil para sua ascensão e propagação dentro da arquitetura Blockchain, cabe salientar que ela não é uma solução destinada somente à troca de moedas virtuais.

Na verdade, a solução garante que o Bitcoin possa circular com sigilo, segurança, rastreabilidade e particularidade. Mas a arquitetura vai além e permite o processamento de registro e transações de todos os fins, sejam eles tangíveis – transações de bens, como um carro, casa e roupas – ou intangíveis – bens de propriedade intelectual.

Desta forma, o Blockchain funciona como um grande livro-razão para as transações bitcoin, transações essas descentralizadas, compartilhadas e executadas em cadeia de blocos.

Com isso, podemos concluir que, no futuro, praticamente qualquer coisa de valor poderá ser negociada dentro da plataforma Blockchain. Com uma grande vantagem e uma mudança cultural muitíssimo relevante e preocupante, não será necessária a necessidade de terceiros e atravessadores.

Figura 1.12 – Transações Bitcoin
Fonte: Shutterstock (2017)

1.4.2 Principais utilizações do Blockchain

- Implementação de contratos inteligentes.
- Armazenamento em clouds distribuídos.
- Identidade digital.
- Votação digital.
- Operações cambiais imediatas.
- Cartórios digitais.
- Registro de patentes.
- Propriedade intelectual.
- Moedas digitais.
- Direito Digital.
- Transações imobiliárias.
- Prontuário médico.
- Gestão Pública.

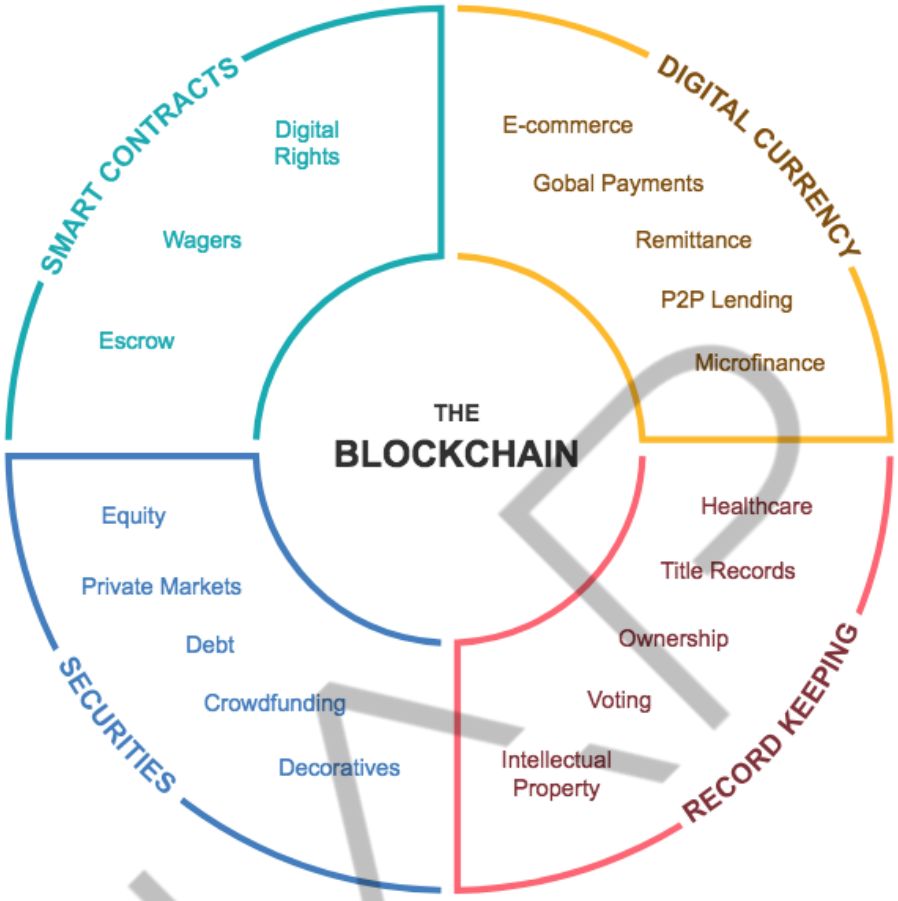

Figura 1.13 – Blockchain impactando indústrias
Fonte: FIAP (2020)

REFERÊNCIAS

CCM. **Introdução à codificação DES**. Disponível em: <http://br.ccm.net/contents/132-introducao-a-codificacao-des>. Acesso em: 20 jul. 2020.

CERQUEIRA, Aurimar Harry; STELER, Fernando Wosniak. **Tudo o que você queria saber sobre blockchain e tinha receio de perguntar.** 6 mar. 2017. Disponível em: <http://computerworld.com.br/tudo-o-que-voce-queria-saber-sobre-blockchain-e-tinha-receio-de-perguntar>. Acesso em: 20 jul. 2020.

GUPTA, Manav. **Blockchain for Dummies**. New Jersey: IBM Limited Edition, 2017.

SIMPLY TECNOLOGIA. **Blockchain:** saiba o que é e como pode ser usado pelos bancos. Disponível em: <http://blog.simply.com.br/blockchain-saiba-o-que-e-e-como-pode-ser-usado/>. Acesso em: 20 jul. 2020.

SIMPLY TECNOLOGIA. **Blockchain**: saiba o que é e como pode ser usado pelos Bancos. 01 jun. 2016. Disponível em: <http://blog.simply.com.br/blockchain-saiba-o-que-e-e-como-pode-ser-usado/>. Acesso em: 20 jul. 2020.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution** – como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: Senai-SP Editora, 2016.