CENTRO DE EDUCAÇÃO SUPERIOR DE BRASÍLIA

INSTITUTO DE EDUCAÇÃO SUPERIOR DE BRASÍLIA

MAURICIO THEODOSIO MATTOS MARQUES

(Matrícula: 1886309027)

TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES NA ÁREA DE TRÂNSITO

Brasília - DF

2019

MAURICIO THEODOSIO MATTOS MARQUES
(Matrícula: 1886309027)

TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES NA ÁREA DE TRÂNSITO

Trabalho de Conclusão de Curso de Pós-Graduação *Lato Sensu* apresentado ao Centro Universitário Instituto de Educação Superior de Brasília – IESB como exigência parcial para a obtenção de título de especialização em Segurança da Informação.

Professor Orientador: Msc. Rozelito Felix da Silva.

Brasília – DF
2019

MAURICIO THEODOSIO MATTOS MARQUES
(Matrícula: 1886309027)

TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES NA ÁREA DE TRÂNSITO

Trabalho de Conclusão de Curso de Pós-Graduação *Lato Sensu* apresentado ao Centro Universitário Instituto de Educação Superior de Brasília – IESB como exigência parcial para a obtenção de título de especialização em Segurança da Informação.

Brasília, 1 de maio de 2019

Banca examinadora:

_____

Professor Orientador: Msc. Rozelito Felix da Silva.

DEDICATÓRIA

Aos meus queridos pais, in memoriam, aos quais devo tudo do pouco que sou e que sei, e que não tiveram tempo de vivenciar mais essa colheita;

À minha família, em particular à minha morena, a quem me ensina cotidianamente que a idade é um estado de espírito, pelo apoio e incentivo incansável, pelas noites de privação do nosso convívio, sempre acreditando valer a pena.

AGRADECIMENTOS

À Deus acima de tudo;

À minha querida esposa Vania Viveiros Montenegro Marques pelo incansável apoio na realização de mais um sonho;

Ao DER/DF, na pessoa do Coordenador de Tecnologia da Informação José Geraldo de Melo, por autorizar a minha dedicação à pesquisa no horário de trabalho;

Ao DER/DF, na pessoa da servidora Larissa Santos Santana, por me apontar as principais dificuldades enfrentadas no órgão com o sistema RENAINF atual;

Ao DETRAN/DF na pessoa do servidor Renan Wilson Lopes Prudêncio; por me apontar as principais dificuldades enfrentadas no órgão com o sistema RENAINF atual;

Ao DENATRAN na pessoa dos servidores Carlos Magno, Abílio da Silva Gomes, Marcela Laiz e Rodrigo Vitorio, por me apontar as principais dificuldades enfrentadas no órgão com o sistema RENAINF atual;

Ao DNIT na pessoa da servidora Izabel Lima Alexandria, por me apontar as principais dificuldades enfrentadas no órgão com o sistema RENAINF atual;

À Presidência da República, na figura do amigo Marco Rosa, que me apresentou a tecnologia Blockchain num encontro num bar;

À PRF na pessoa do servidor Vinícius Medeiros, por me apontar as principais dificuldades enfrentadas no órgão com o sistema RENAINF atual;

Ao SERPRO na figura dos profissionais envolvidos com o Sistema RENAINF: Anderson Roberto Germano, Carlos Magno Arantes, Felipe Lopes da Silva, Gleison Tavares Diolino, José Antônio de Almeida e Marco Túlio da Silva Lima;

Ao meu orientador Msc. Rozelito Felix da Silva, pelo apoio e incentivo desde o início do curso. Você fez toda a diferença.

RESUMO

TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES NA ÁREA DE TRÂNSITO

Autor: Mauricio Theodosio Mattos Marques
Orientador: Msc. Rozelito Felix da Silva
Programa de Pós-Graduação Lato Sensu em Segurança da Informação
Brasília, 01 de Maio de 2019.

O presente trabalho aborda os fundamentos teóricos e funcionamento da tecnologia Blockchain e procura mostrar como ela pode ser utilizada para elevar o nível de segurança, confiabilidade e transparência nas ações governamentais, particularmente na área de trânsito. Por se tratar de uma tecnologia relativamente recente, há poucos trabalhos acadêmicos voltados para esta temática, como também há uma grande necessidade de familiarização com a tecnologia nos meios acadêmicos, mercadológicos e governamentais, especificamente no poder legislativo onde o assunto carece de uma regulamentação específica, a exemplo do que já ocorre em alguns países. A metodologia utilizada no trabalho, buscando facilitar o entendimento do leitor, foi a segmentação em 3 (três) fases a saber:

- **Pesquisa:** fase em que se abordam os conceitos básicos e a fundamentação teórica da tecnologia Blockchain;
- **Aplicação:** fase de prospecção de potenciais aplicações da tecnologia Blockchain na área de trânsito;
- **Proposta:** fase em que se propõe uma aplicação da tecnologia Blockchain no processo de gestão de arrecadação das infrações de trânsito em nível nacional.

Ao final do trabalho é abordado o porquê a tecnologia Blockchain é adequada para o setor público, e como isto pode ser alcançado.

Palavras Chave: Tecnologia Blockchain. Criptografia Assimétrica. Funcão de Hash. Sistemas Distribuídos. Transparência Pública.

ABSTRACT

TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES NA ÁREA DE TRÂNSITO

Author: Mauricio Theodosio Mattos Marques
Supervisor: Msc. Rozelito Felix da Silva
Programa de Pós-Graduação Lato Sensu em Segurança da Informação
Brasília, May 1, 2019

This paper deals with the theoretical foundations and operation of Blockchain technology and seeks to show how it can be used to raise the level of security, reliability and transparency in government actions, particularly in the area of traffic. Because it's a relatively recent technology, there are few academic papers focused on this subject, as there is a great need for familiarization with technology in the academic, marketing and government sectors, specifically in the legislative branch where the subject needs specific regulation, as it's already the case in some countries. The methodology used in the work, seeking to facilitate the understanding of the reader, was the segmentation in 3 (three) phases namely:

- **Research:** phase in which the basic concepts and the theoretical foundation of Blockchain technology are addressed;
- **Application:** prospecting phase of potential applications of Blockchain technology in the transit area;
- **Proposal:** phase in which it's proposed to apply Blockchain technology in the process of managing the collection of traffic infractions at the national level.

At the end of the paper is discussed why Blockchain technology is suitable for the public sector, and how this can be achieved.

Keywords: Blockchain Technology. Asymmetric Cryptography. Hash function. Distributed systems. Public Transparency.

LISTA DE FIGURAS E TABELAS

LISTA DE FIGURAS E TABELAS

LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIAÇÕES

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AIT	Auto de Infração de Trânsito
ANTT	Agência Nacional de Transportes Terrestres
B2B	Business to Business
BIN	Base Índice Nacional
BINCO	Base Índice de Condutores
BINIT	Base Índice Nacional de Infrações de Trânsito
CCE	Criptografia de Curvas Elípticas
CETRAN	Conselho Estadual de Trânsito
CF	Constituição Federal
CNH	Carteira Nacional de Habilitação
CONTRAN	Conselho Nacional de Trânsito
CONTRANDIFE	Conselho de Trânsito do Distrito Federal
CPF	Cadastro de Pessoas Físicas
CTB	Código de Trânsito Brasileiro
CVM	Comissão de Valores Mobiliários
DAPPS	Decentralized Applications
DBFT	Delegated Bizantine Fault Tolerance
DENATRAN	Departamento Nacional de Trânsito
DER/DF	Departamento de Estradas de Rodagem do Distrito Federal
DETRAN/DF	Departamento de Trânsito do Distrito Federal
DLT	Distributed Ledger Tecnology
DNIT	Departamento Nacional de Infraestrutura de Transportes
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECC	Elliptic Curves Cryptography

LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIAÇÕES

ECDSA	Elliptic Curve Digital Sgnature Algorithm
EV01	Evento de Transação de Envio 01
EVM	Ethereum Virtual Machine
FUNSET	Fundo Nacional de Segurança e Educação de Trânsito
GRU	Guia de Recolhimento da União
IDEA	International Data Encryption Algorithm
IDS	Intrusion detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
JARI	Junta Administrativa de Recursos de Infrações
MVP	Mínimo Produto Viável
NA	Notificação de Autuação
NP	Notificação de Penalidade
NSA	National Security Agency
OA	Órgão Arrecadador do RENAINF
OCD	Órgão Coordenador Distrital do RENAINF
OCE	Órgão Coordenador Estadual do RENAINF
OCG	Órgão Coordenador Geral do RENAINF
P2P	Peer-to-Peer
PIN	Personal Indentification Number
PM	Polícia Militar
PoC	Proof of Concept
PoW	Proof of Work
PoS	Proof of Stake
PRF	Departamento de Polícia Rodoviária Federal
RC4	Rivest Cipher 4
RFB	Receita Federal do Brasil

LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIAÇÕES

RENACH	Registro Nacional de Carteiras de Habilitação
RENAINF	Registro Nacional de Infrações de Trânsito
RENAVAM	Registro Nacional de Veículos Automotores
RSA	Rivest-Shamir-Adleman
RT01	Evento de Transação de Retorno 01
SERPRO	Serviço Federal de Processamento de Dados
SHA-256	Secure Hash Algorithm
SNE	Sistema de Notificação Eletrônica
SNT	Sistema Nacional de Trânsito
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOD	Transaction Ordering Dependence
UF	Unidade da Federação
UTXO	Unspent Transaction Output

SUMÁRIO

1 INTRODUÇÃO

Quando a Internet surgiu, muita gente não tinha ideia do que fazer com esse novo invento. Hoje em dia, você se imagina sem ela? Mark Zuckerberg, o criador do Facebook, certa vez definiu a Internet como "um campo aberto e pouco explorado". O fato é que nas últimas quatro décadas, presenciamos o surgimento do e-mail, da Word Wide Web, das empresas .com, das mídias sociais, da internet móvel, do Big Data, da computação em nuvem, da inteligência artificial e dos primórdios da Internet das coisas. Até agora, o poder transformador da rede mundial tem sido estonteante. Constatamos empresas surgirem e sumirem numa velocidade nunca vista antes. Alguns exemplos desta transformação são notórios, como na indústria de Áudio (Spotify, iTunes), na de Vídeo (Netflix), na de Transporte (Uber), na de serviços on-line e de software (Google), nas redes sociais (Facebook, Twitter, Instagram, Google+, Youtube, MySpace, Badoo, Likedin, Tinder), no mercado Imobiliário (Airbnb,), no turismo (Booking, Trivago) e no Financeiro (Fintechs). Diante destes acontecimentos, nos perguntamos: O que ainda está por vir? Para muitos analistas, já existe uma tecnologia disruptiva em plena ascensão na Internet capaz de provocar novas e grandes transformações em vários setores simultaneamente, como o de Infraestrutura, Financeiro, de Medicina, de Logística, de Governo, de Identificação Pessoal, dentre outros. Trata-se de uma tecnologia chamada de Blockchain. Há quem diga que estamos diante de uma segunda era da economia digital. Enquanto a primeira foi caracterizada pela convergência entre tecnologias da computação e da comunicação, a segunda seria decorrente de uma combinação de engenharia computacional, matemática, criptografia e economia comportamental [Tapscott, 2016]. Sua adoção será gradual, começando com desenvolvedores e empreendedores de startups, em seguida por pessoas de negócios tecnológicos e organizações que veem a mudança, e então pela sociedade, chegando finalmente às organizações que antes eram resistentes a ela. O seu crescimento tem uma vantagem em relação a trajetória de evolução da Web, pois seu ponto de partida é amplificado por quatro segmentos: usuários da web, usuários de telefones celulares, proprietários de sites e "qualquer coisa" que se beneficiar de estar conectada e se tornar algo sagaz [Mougayar, 2017]. Prevê-se um impacto sobre todas as funções e atividades da indústria de serviços financeiros, mas certamente isto é apenas uma das inúmeras possíveis aplicações desta tecnologia, que certamente terá um longo caminho pela frente. Segundo a revista inglesa The Economist, a tecnologia Blockchain é *"a grande cadeia de certeza sobre as coisas"*. É esperar para ver.

1.1. MOTIVAÇÃO

Muito se tem falado e escrito sobre essa tecnologia que permite transações e registros sem intermediários, um protocolo de confiança, um banco de dados público, descentralizado e distribuído, uma rede de pagamentos de baixo custo, altamente segura e semianônima. A tecnologia Blockchain está atraindo grande atenção da comunidade tecnológica mundial, seu projeto original datado de 2008 com a publicação do artigo *"Bitcoin: A Peer-to-Peer Eletronic Cash System"* por Satoshi Nakamoto, tem servido de inspiração para o surgimento de inúmeras aplicações, e hoje já existem vários projetos em diferentes segmentos como rastreamento de ativos, comprovação e validação de identidades, Internet das coisas, governo, dentre outras. No entanto, o setor financeiro ainda é visto como o seu usuário principal, dada a popularidade do Bitcoin criptomoeda, onde o Blockchain é a sua tecnologia subjacente.

Em função do potencial de sua aplicação, há muito ainda a se familiarizar com a tecnologia Blockchain: Academia, Mercado e Governo devem se aprofundar em estudos e experimentos no tema. É necessário que se conheçam os riscos e oportunidades envolvidos, a fim de que se descortine a tão falada "Revolução Digital" onde essa tecnologia promete superar aspectos críticos de intermediação, representando *"uma mudança de confiar em pessoas para confiar em matemática"* [Antonopoulos, 2014] e que *"devemos abrir nossa mente e aceitar que a confiança será computada por máquinas, e não verificadas por humanos"* [Mougayar, 2017], uma vez que a tecnologia Blockchain se baseia em criptografia avançada para garantir segurança em suas transações, além do que, há uma tendência de que as intervenções humanas em aplicações serão cada vez menos necessárias.

Como Servidor Público do Departamento de Estradas de Rodagem do Distrito Federal (DER/DF), uma Autarquia Rodoviária, de Trânsito e de Mobilidade, atuando no setor desde 1991, entendo que a tecnologia Blockchain pode ser de grande valia na superação de dificuldades hoje existentes, como por exemplo na otimização do processo de organização e manutenção das bases de dados do Departamento Nacional de Trânsito (DENATRAN), conforme preconiza o Código de Trânsito Brasileiro (CTB) em seu artigo 19, incisos VIII, IX e XXX.

O uso da tecnologia Blockchain promete trazer eficiência significativa para cadeia de suprimentos globais, transações financeiras, contagem de ativos e redes sociais descentralizadas. Prever o impacto desta tecnologia não é tarefa nada fácil, e a única certeza que se tem é a de que a partir dela, "nada será como antes", basta olharmos para a história recente da Internet. Quem viver verá.

1.2. OBJETIVOS

Os principais objetivos deste trabalho podem ser sintetizados em:

a) Apresentar o funcionamento da tecnologia Blockchain, na sua essência, como base para as mais diversas aplicações;

b) Avaliar casos de aplicação da tecnologia Blockchain para o provimento da transparência na Gestão Pública;

c) Indicar possíveis implementações de aplicações que podem ser usadas no âmbito da Administração Pública, particularmente na área de trânsito, visando prover maior confiabilidade e transparência;

d) Propor um caso prático de registro de arrecadação de infrações de trânsito, que demonstre a efetividade da tecnologia Blockchain.

Pretende-se assim, como objetivo maior deste trabalho, considerando o estado da arte do Blockchain, mostrar o enorme potencial desta tecnologia, com aplicações na Administração Pública, conferindo-lhe, com isso, maior nível de transparência e confiabilidade.

1.3. METODOLOGIA

A metodologia de pesquisa proposta foi dividida em 4 (quatro) fases com o propósito de facilitar o entendimento do trabalho, conforme apresentado a seguir:

a) **Fase 1 - Pesquisa teórica:** fase em que se aborda os conceitos básicos e o funcionamento da tecnologia Blockchain, com base na leitura e análise de publicações relevantes ao trabalho, com o objetivo de dar sustentação teórica para o estudo desenvolvido nas demais fases;

b) **Fase 2 - Pesquisa por casos de uso na utilização da tecnologia:** fase de prospecção de potenciais aplicações da tecnologia Blockchain relacionadas à área de trânsito;

c) **Fase 3 - Estudo de um caso prático:** fase em que se procura reproduzir, em menor escala, os efeitos de uma aplicação da tecnologia Blockchain num dos cenários abordados na fase anterior;

d) **Fase 4 - Estudo de aplicações futuras:** fase de prospecção de outras possíveis aplicações da tecnologia Blockchain na área de trânsito.

1.4. ORGANIZAÇÃO DO TRABALHO

O trabalho está dividido em 5 (cinco) capítulos a saber:

a) **Capítulo 1 (Introdução):** Aborda os principais objetivos do trabalho, a metodologia empregada bem como a sua organização;

b) **Capítulo 2 (Estado da Arte e Revisão da Literatura):** Aborda os conceitos básicos ligados à tecnologia Blockchain, o seu funcionamento, contratos inteligentes, suas variações, questões de segurança envolvidos, padrões genéricos de aplicações, casos de uso e os obstáculos e desafios relacionados à sua implementação;

c) **Capítulo 3 (Aplicação do Blockchain na área de Trânsito):** Aborda alguns aspectos da legislação de trânsito brasileira e as características de 3 (três) bases de dados mantidas pelo DENATRAN: o Registro Nacional de Infrações de Trânsito (RENAINF), o Registro Nacional de Carteiras de Habilitação (RENACH) e o Registro Nacional de Veículos Automotores (RENAVAM)

d) **Capítulo 4 (Simulação de Registro de Arrecadação de Infrações):** Aborda uma aplicação da tecnologia Blockchain, na organização e manutenção do Registro Nacional de Infrações de Trânsito (RENAINF);

e) **Capítulo 5 (Considerações Finais):** Aborda a prospecção de outras possíveis aplicações da tecnologia Blockchain na área de trânsito.

2 ESTADO DA ARTE E REVISÃO DA LITERATURA

Para facilitar o entendimento do trabalho, este capítulo foi dividido em 8 (oito) seções procurando apresentar, de uma forma estruturada, o estado da arte envolvendo a tecnologia Blockchain.

2.1. CONCEITOS BÁSICOS

Esta seção apresenta a fundamentação teórica na qual a tecnologia Blockchain foi concebida e está estruturada.

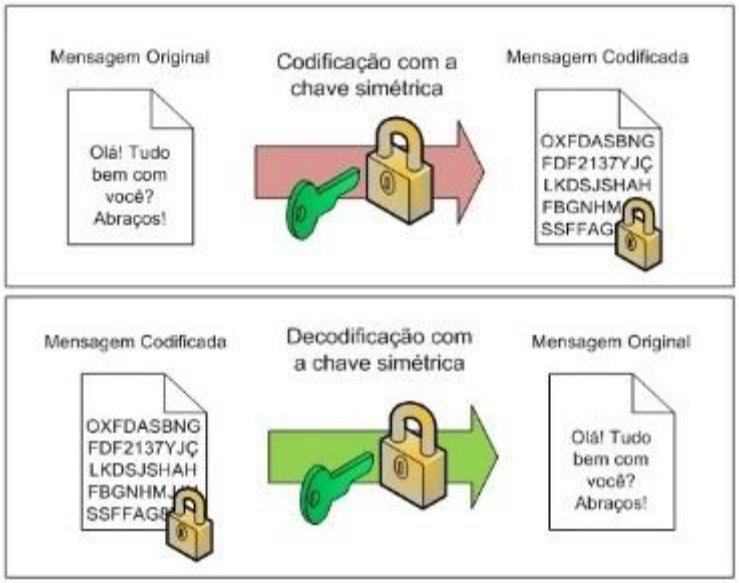
2.1.1. Criptografia

Segundo a Cartilha de Segurança para a Internet, editada pelo Comitê Gestor de Internet no Brasil (2012), a criptografia é a ciência e a arte de escrever mensagens em forma cifrada ou em código. De acordo com o tipo de chave usada na codificação dos dados, os métodos criptográficos podem ser subdivididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

2.1.1.1. Criptografia de chave simétrica

Também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave (Figura 2.1) tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Trata-se da forma mais antiga de criptografia, e seu principal inconveniente reside no fato de demandar um canal seguro para o compartilhamento da chave secreta entre os seus usuários. Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

Figura 2.1 - Criptografia de chave simétrica.

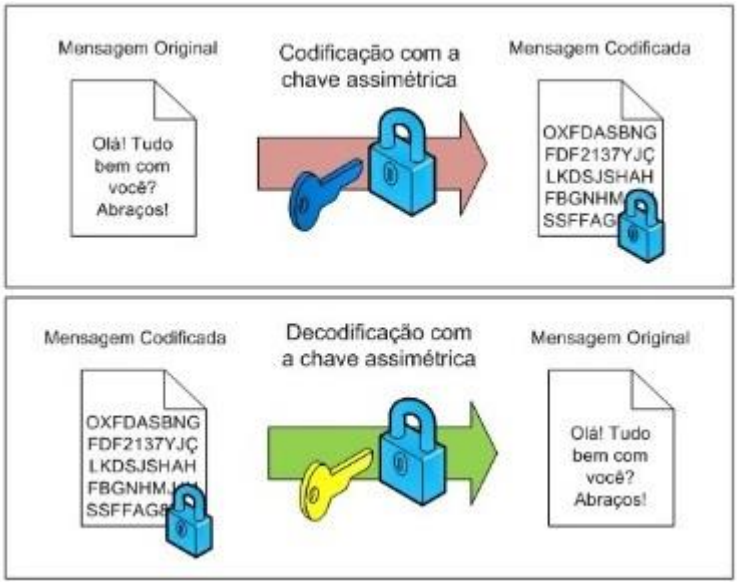


Fonte: (Carvalho, 2008, adaptado).

2.1.1.2. Criptografia de chaves assimétricas

Também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu proprietário (Figura 2.2). Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio. É considerada mais segura e mais lenta do que a criptografia simétrica, devido a sua complexidade algorítmica. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

Figura 2.2 - Criptografia de chave assimétrica.



Fonte: (Carvalho, 2008, adaptado).

A segurança de um sistema criptográfico assimétrico está na diferença entre o caminho de ida e o caminho de volta da operação matemática em que a criptografia está fundamentada [Impagliazzo, 1989]. Quanto maior esta diferença, mais eficiente o algoritmo. Diffie-Hellman, um dos primeiros algoritmos a fazer uso de assimetria em criptografia, baseia-se na dificuldade de se reverter operações logarítmicas e é normalmente utilizado para acordo de uma chave privada. RSA, cujo nome remete às iniciais de seus inventores – Rivest, Shamir e Adleman – explora a dificuldade de se fatorar um número em fatores primos, comparado a facilidade de multiplicar dois primos para gerar um produto. Atualmente, a Criptografia de Curvas Elípticas (CCE) é considerada a mais eficiente, além de ser a mais utilizada para aplicações da tecnologia Blockchain, pois requerem chaves menores (256 bits em vez de 2048 bits do RSA, em média). A Criptografia CCE é baseada nas propriedades matemáticas das curvas elípticas, descritas pela seguinte equação:

$$Y^2 = X^3 + aX + b$$

Segundo [Miller, 2017], na tecnologia Blockchain, usando o método Elliptic Curve Digital Sgnature Algorithm (ECDSA), em sua especificação secp256k1, os endereços (chaves públicas) são obtidos a partir de uma chave privada (número gigante) gerada aleatoriamente, normalmente através de softwares que utilizam funções do próprio sistema operacional. Considerando que é com a chave privada que as operações serão assinadas e valores serão

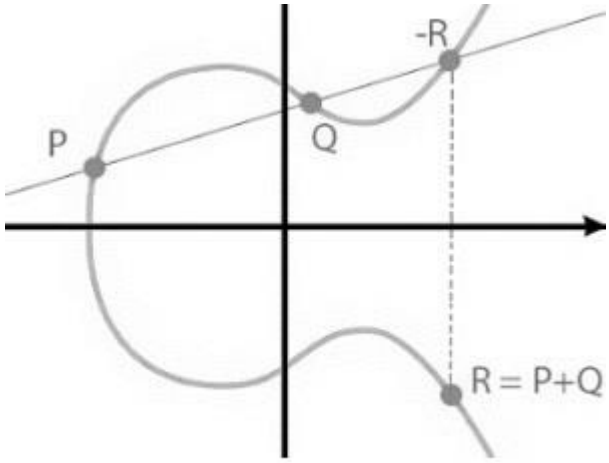
transferidos na rede, mantê-la de uma forma segura é essencial para segurança das transações na tecnologia Blockchain [Agner, 2018]. A chave pública (K) é obtida então a partir da multiplicação de um ponto base da curva (G) pela chave privada (k). Este ponto base é público, determinado pela especificação e nunca muda.

$$K = G * k \text{ (Chave pública = Ponto base * Chave privada)}$$

Para a obtenção da Chave pública, o ECDSA usa uma série de operações aritméticas especiais em pontos de uma curva elíptica, a partir de repetidas operações de adição de coordenadas polares, obtidas pela interseção da curva elíptica com diversas retas tangentes. Para isso, dois tipos de operações são usados no processo: a adição e a multiplicação de pontos na curva.

a) **Adição de pontos na curva elíptica [Miller, 2017]:** partindo de dois pontos da curva elíptica (vamos chamá-los de P e Q), desenhamos uma linha que cruzará (nem sempre) com a mesma em um ponto que chamaremos de -R. Para se obter então a soma de P + Q, será suficiente refletir o ponto -R no eixo X e, assim, chegar ao ponto R que será a soma geométrica de P + Q (Figura 2.3).

Figura 2.3 - Adição de pontos na curva elíptica.

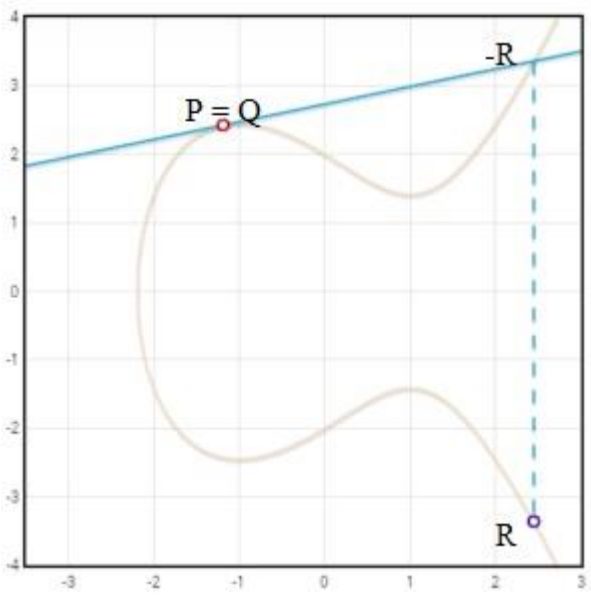


Fonte: (Miller, 2017, adaptado).

b) **Multiplicação de pontos na curva elíptica [Miller, 2017]:** a multiplicação, nada mais é do que adicionar um mesmo valor a ele mesmo "n" vezes. Já vimos anteriormente o cálculo de R

como a soma de P e Q quando P e Q são pontos diferentes: P + Q = R, consequentemente, quando P e Q é o mesmo ponto: P + P = 2P = R. Portanto, se usássemos mais de dois pontos iguais para obter R, o cálculo seria: P + P + P + P + P +P+... + P = nP. Graficamente falando, quando P e Q é o mesmo ponto, não podemos traçar uma linha para obter R, então recorremos à tangente do ponto P para obter a linha de que precisamos. Como P = Q, então P + Q = 2P = R (Figura 2.4).

Figura 2.4 - Multiplicação de pontos na curva elíptica.



Fonte: (Miller, 2017, adaptado).

No caso do padrão de curva elíptica especificada na secp256k1, usado pelo Bitcoin, a equação $Y^2 = X^3 + aX + b$ é definida como:

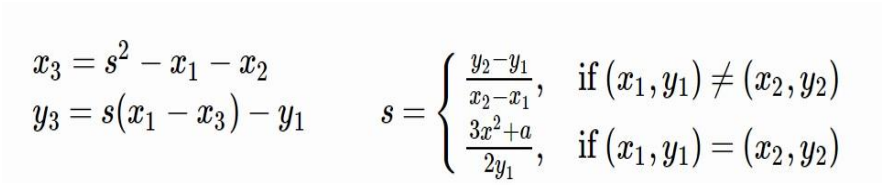
$$Y^2 = X^3 + 7 \pmod{p}$$

Sendo que, o mod p (módulo de um determinado número primo) indica que essa curva está sobre um campo finito de números primos p, onde p é o limite do campo finito de números inteiros utilizados na curva, cujo valor é definido como sendo $2^{256} – 2^{32} – 977$. A razão para se escolher este número é que ele é primo, seu comprimento é de 256 bits e sua expressão binária tem 127 (cento e vinte e sete) “zeros” e 129 (cento e vinte e nove) “uns”, o que facilita os cálculos [Miller, 2017].

A fórmula aritmética desse tipo de soma (para obter R de P e Q) é a seguinte (Figura 2.5):

Dado (x1, y1), (x2, y2) devemos encontrar (x3, y3) = (x1, y1), (x2, y2)

Figura 2.5 - Fórmula aritmética da soma de pontos na curva elíptica.



$$x_3 = s^2 - x_1 - x_2$$
$$y_3 = s(x_1 - x_3) - y_1$$
$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } (x_1, y_1) \neq (x_2, y_2) \\ \frac{3x^2 + a}{2y_1}, & \text{if } (x_1, y_1) = (x_2, y_2) \end{cases}$$

Fonte: (Miller, 2017, adaptado).

c) **Cálculo das chaves privada e pública [Miller, 2017]:** a chave privada k será um número inteiro, selecionado aleatoriamente, entre aqueles que fazem parte do grupo ou corpo finito que definimos, no nosso caso um número entre 1 e p-1, onde p no caso do padrão de curva elíptica secp256k1, usado pelo Bitcoin, é um número primo enorme, a saber:

p=115792089210356248762697446949407573530086143415290314195533631308867097853951

A chave pública, como já visto, é o ponto K obtido pela multiplicação da chave privada k pelo ponto base G.

K = G * k (Chave pública = Ponto base * Chave privada)

Lembrando que o ponto base G (também chamado ponto gerador) é sempre o mesmo ponto (G_x,G_y) para todas as chaves públicas a serem calculadas, e é dado pela especificação secp256k1 usada no protocolo Bitcoin como: [Agner, 2018]

G_x=55066263022277343669578718895168534326250603453777594175500187360389116729240

G_y=32670510020758816978083085130507043184471273380659243275938904335757337482424

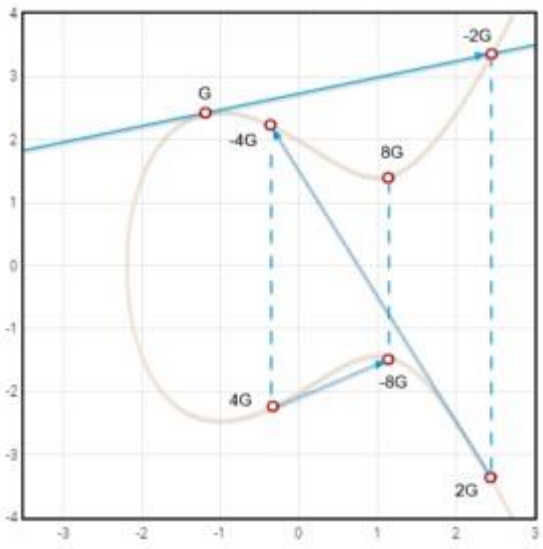
Assim, é uma questão de multiplicar um ponto na curva elíptica, ou adicionar o ponto básico G na curva k vezes, aplicando o procedimento de soma dos pontos visto acima. O ponto base (G) seria o ponto P naquela primeira curva, aquela que usava números reais em

vez de números inteiros, que é o que usaremos para visualizá-lo melhor. Graficamente falando (Figura 2.6), o processo então seria o seguinte:

1. Desenhamos a tangente de G (que é o ponto P);
2. O ponto que corta a curva é o ponto -2G que refletimos no eixo X para se chegar ao ponto 2G;
3. Traçamos a tangente de 2G;
4. O ponto que corta a curva é o ponto -4G que refletimos no eixo X para se chegar ao ponto 4G;
5. Traçamos a tangente de 4G;
6. O ponto que corta a curva é o ponto -8G que refletimos no eixo X para se chegar ao ponto 8G.

Esse processo é então repetido até chegarmos a kG e obter as coordenadas de K (kG = K) que será a nossa chave pública.

Figura 2.6 - Multiplicação de pontos na curva elíptica.



Fonte: (Miller, 2017, adaptado).

De todo o exposto, [Miller, 2017] ainda destaca os seguintes pontos:

- A chave privada é apenas um número aleatório no qual podemos realizar cálculos matemáticos normais;

- A chave pública, em vez disso, é um ponto em uma curva elíptica na qual somente as operações de adição e multiplicação podem ser executadas, mas não podem ser divididas;

- É fácil calcular a chave pública usando o sistema de multiplicação escalar e praticamente impossível obter a chave privada pela força bruta;

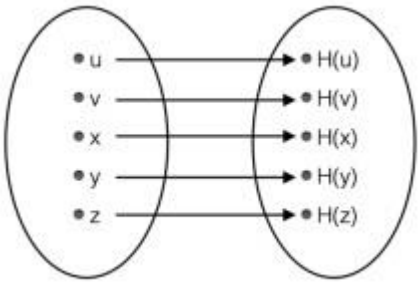
- É muito importante que a chave privada seja aleatória. A maioria dos problemas de segurança detectados até agora se deve a uma implementação deficiente ao se gerar a chave privada, abordado na seção 2.5 (Questões de Segurança).

É importante ressaltar que uma chave criptográfica possui a propriedade de decriptografar a mensagem criptografada pela sua chave correspondente. Tanto a chave pública quanto a chave privada podem ser usadas para criptografar uma mensagem, dependendo da finalidade para a qual a criptografia é utilizada. De modo geral, a criptografia com a chave pública provê confidencialidade, enquanto a criptografia com a chave privada provê autenticidade. Esta ideia deve ficar mais clara na seção 2.1.3, onde é apresentado o conceito de assinatura digital.

2.1.2. Função de Hash

Uma função de Hash, ou função de resumo, é também conhecida como Message Digest. É um método criptográfico que, quando aplicado sobre uma informação, independentemente do seu tamanho, gera um resultado único e de tamanho fixo (*Digest*), razão pela qual é considerada a impressão digital de um dado. Uma vez gerado o Hash, não é possível realizar o processamento inverso para se obter a informação original (Figura 2.7). Assim, a função de Hash pode ser utilizada para:

Figura 2.7 - Função.



Fonte: (Pires, 2016, adaptado).

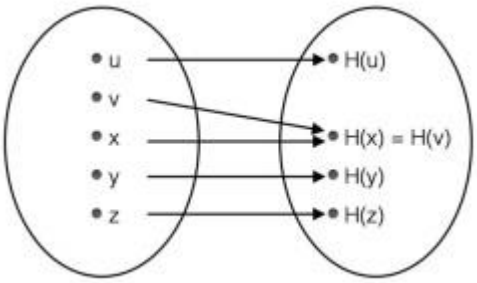
a) **Verificação da integridade de dados:** aplica-se a função de Hash diretamente sobre o dado original e se salva o resumo gerado. Após o dado ser transmitido para o receptor, este calcula o resumo sobre o dado recebido e obtém um novo resumo. Se os resumos forem iguais, assume-se que o dado está integro. Este é o método utilizado para geração de assinaturas digitais, a ser abordado na próxima seção;

b) **Armazenamento de senhas de segurança:** o processo é semelhante ao anterior, ou seja, ao se cadastrar uma senha, armazena-se apenas o resumo da senha. No processo de autenticação, quando o usuário fornece sua senha, calcula-se a função de Hash da senha fornecida e se compara com o resumo previamente armazenado. Se os resumos forem iguais, o usuário é autenticado;

c) **Busca de elementos em bases de dados:** nas bases de dados estruturadas em índices, os mesmos são baseados em Hashs, onde a busca pela página da informação é feita pelo resumo e não pelo dado. Em geral, calcula-se o resumo do dado e, com o resumo, sabe-se em que página o dado está. Assim, não precisamos varrer todo o índice para descobrir a página em que o dado se encontra.

Existem diversos tipos de função resumo e a sua complexidade depende, basicamente, das propriedades que se deseja garantir. A propriedade básica de todas as funções resumo é a de ser unidirecional, ou seja, não é possível recuperar o dado original a partir do resumo gerado. Um exemplo de função resumo é a função resto da divisão. Digamos que utilizamos a função resto pela divisão por 5 (cinco). Assim, todos os números da sequência 1, 6, 11, 16, 21, … terão o resumo igual a 1 (um). Nesse caso, dado que se tem o mesmo resumo 1, não é possível se identificar qual número o gerou. Essa repetição de resumos leva à segunda propriedade de todas as funções de Hash que é a colisão. Quando dois ou mais dados originais geram o mesmo resumo, tem-se uma colisão (Figura 2.8). O mecanismo mais utilizado para se reduzir a probabilidade de ocorrência das colisões é o ajuste da distribuição dos resumos. Quanto mais uniforme e dispersa é a função resumo, menor é a sua probabilidade de colisão. Um exemplo de função bastante uniforme é a função resto pela divisão por 5 (cinco), do exemplo citado anteriormente. Cada um dos valores possíveis de resultado da função é gerado pela mesma quantidade de números. No entanto, a função resto não possui boa dispersão dos resumos gerados, ou seja, os resumos de números próximos são bem próximos. Como os dados a serem resumidos tendem a ter alguma correlação, funções com baixa dispersão aumentam a probabilidade de colisões na aplicação.

Figura 2.8 - Colisão.



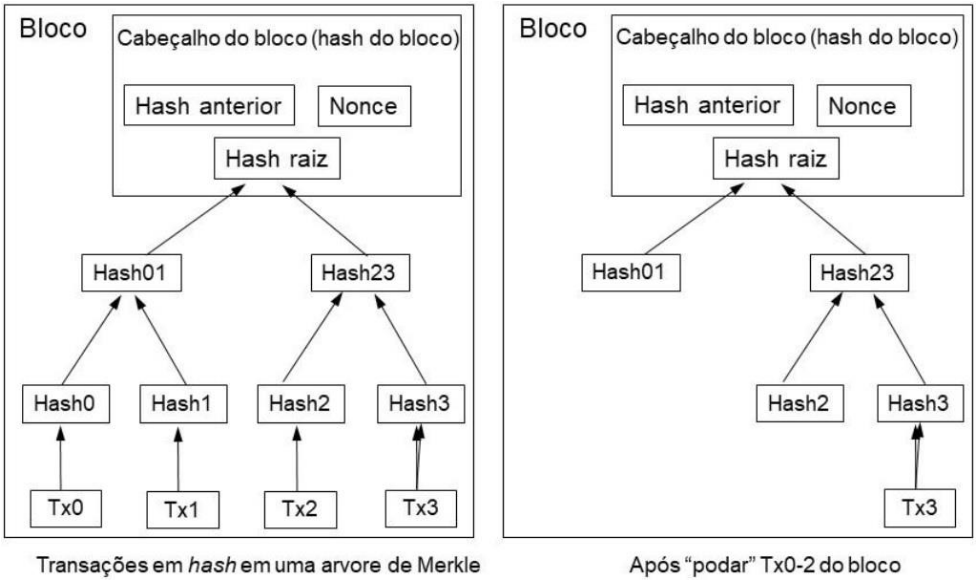
Fonte: (Pires, 2016, adaptado).

Podemos então, definir uma boa função de resumo H(x) como aquela que possui as seguintes características:

- H(x) pode ser aplicada a um bloco de dados de qualquer tamanho;
- H(x) produz uma única saída de comprimento fixo;
- H(x) é relativamente fácil de se calcular para qualquer x, tornando as implementações de hardware ou software práticas;
- Para qualquer h, é computacionalmente inviável encontrar x, tal que H(x) = h (resistência à primeira inversão ou propriedade unidirecional);
- Para qualquer x, é computacionalmente inviável encontrar y diferente de x, tal que H(y) = H(x) (resistência à segunda inversão ou resistência fraca a colisões);
- É computacionalmente inviável encontrar (x, y) tal que H(x) = H(y) (resistência forte a colisões).

A principal implementação de função de Hash utilizada pela tecnologia Blockchain é a Secure Hash Algorithm (SHA-256), projetada pela Agencia Nacional de Segurança dos EUA (NSA). O Hash produzido nessa implementação tem um tamanho fixo de 256 (duzentos e cinquenta e seis) bits. Uma análise mais detalhada do seu funcionamento pode ser encontrada em [Carvalho, 2001]. Uma das principais utilizações da função de Hash na tecnologia Blockchain reside na construção de árvores de Merkle (árvores binárias de Hash). A árvore é construída das folhas para a raiz, realizando o Hash por pares de transações. Quando há um número ímpar de folhas, a última folha é duplicada e hasheada consigo mesma (Figura 2.9). Esta estrutura permite uma rápida verificação das entradas iniciais da função, e reduz em um único Hash a representação de todas as entradas (a raiz da Árvore de Merkle ou Merkle Root). Este mecanismo será mais bem detalhado na seção 2.2 (Funcionamento do Blockchain).

Figura 2.9 - Árvore de Merkle.



Fonte: (Abreu, 2017).

2.1.3. Assinatura Digital

Segundo [Pires, 2016], trata-se de um procedimento criptográfico, que simula uma assinatura, o qual é tratado como substituto à assinatura convencional, uma vez que atende a 2 (duas) propriedades fundamentais de uma assinatura convencional:

a) **Autenticidade:** qualquer pessoa pode saber quem fez a assinatura, mas apenas o seu autor deve saber fazê-la;

b) **Endosso:** a assinatura deve estar vinculada a informação que se pretende endossar e a nenhuma outra.

A utilização da assinatura digital garante as seguintes propriedades da Segurança da Informação durante a transmissão/recepção de uma mensagem:

a) **Autenticidade:** o receptor deve poder confirmar que a assinatura foi feita pelo emissor;

b) **Integridade:** qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento;

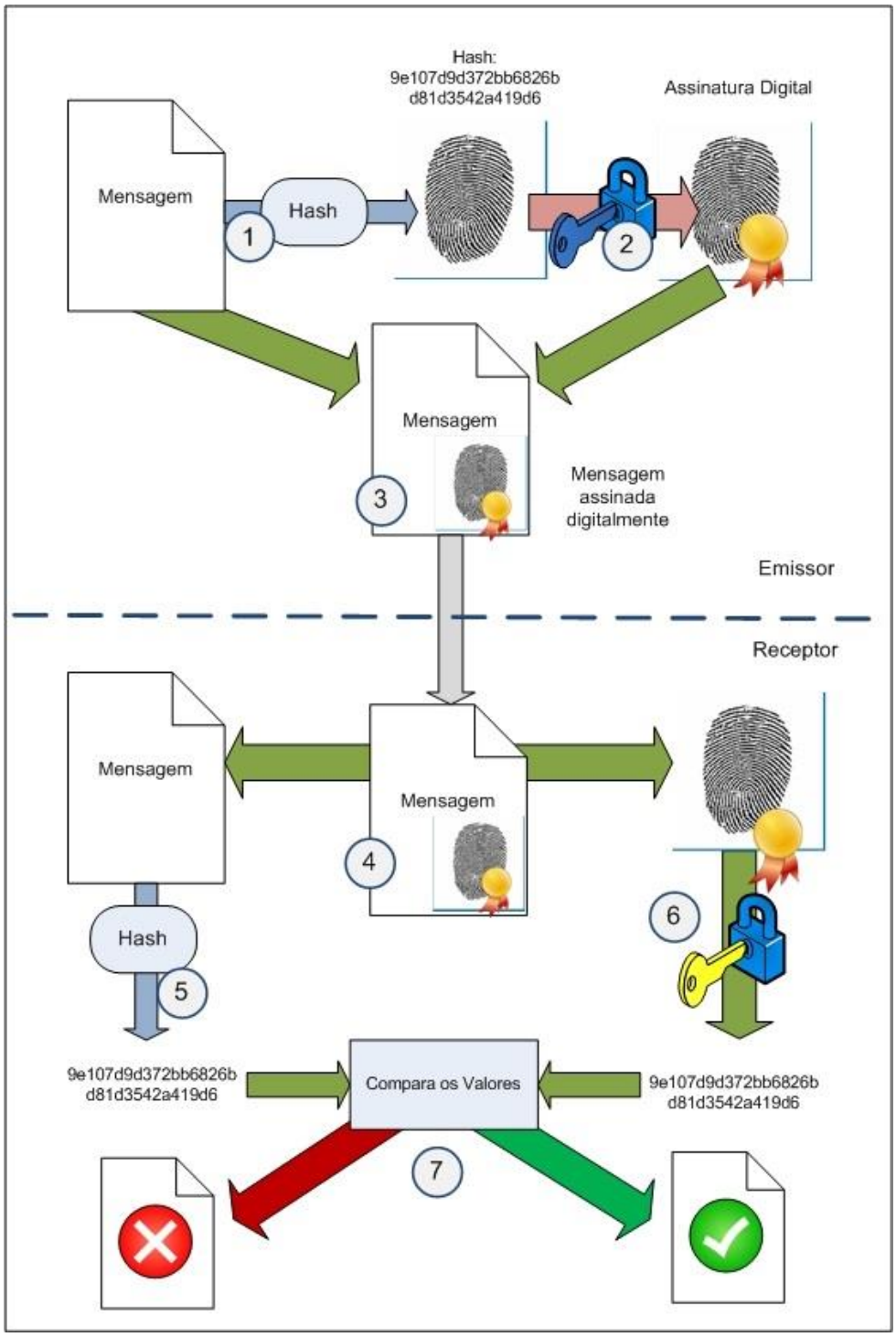
c) **Irretratabilidade ou não-repúdio:** o emissor não pode negar a autenticidade da mensagem.

Como podemos verificar a assinatura digital não garante a confidencialidade da informação. Basicamente, uma assinatura digital típica envolve dois processos criptográficos: o hash do documento a ser assinado, e a encriptação deste hash.

A Figura 2.10 ilustra este processo de assinatura e verificação, onde o emissor gera um hash da mensagem (1), codifica este hash com sua chave privada (2), combina esta assinatura digital com a mensagem e a envia (3). O receptor recebe a mensagem (4) e calcula o hash dela (5). Enquanto isso, ele utiliza a chave pública do emissor para decodificar a assinatura e obter o hash contido na assinatura digital (6). O receptor compara os valores dos hashs (7). Caso os valores sejam idênticos o receptor pode inferir que a mensagem não foi modificada desde a sua emissão. Além disso, a mensagem realmente veio do emissor, pois só ele possui a chave privada que foi utilizada para assinar digitalmente a mensagem. E ao mesmo tempo, o emissor não pode negar que enviou a mensagem, afinal ele a assinou com sua chave privada. Neste exemplo, o objetivo foi a autenticidade e não a confidencialidade, pois a informação estará visível para qualquer pessoa que possuir a chave pública do emissor.

Na tecnologia Blockchain, a essência é a transparência e a visibilidade pública, não há a necessidade de se prover a confidencialidade e sim a autenticidade das transações. É fundamental que cada registro do Blockchain seja manipulado apenas pelas pessoas credenciadas a fazê-lo, onde a criptografia normalmente é aplicada como assinatura e não como encriptação de mensagens. Este mecanismo será melhor detalhado na seção 2.2 (Funcionamento do Blockchain). O algoritmo utilizado para gerar o par de chaves que assina e verifica a mensagem é o ECDSA já abordado na seção 2.1.1 (Criptografia). Para se ter uma noção do alto nível de segurança que este processo provê, a curva elíptica utilizada na tecnologia Blockchain do Bitcoin é a secp256k1, com tamanho de chave de 128 (cento e vinte e oito) bits, ou seja, a dificuldade para se quebrar um par de chaves, neste caso, é de aproximadamente 2^{128} operações de criptografia simétrica [Pires, 2016].

Figura 2.10 - Assinatura Digital.



Fonte: (Carvalho, 2008, adaptado).

2.1.4. Timestamp

Segundo a Wikipédia, timestamp, ou carimbo do tempo, é uma sequência de caracteres ou informações codificadas que identificam quando um determinado evento ocorreu, geralmente fornecendo data e hora do dia, às vezes com precisão de uma pequena fração de segundos. O termo deriva de carimbos usados em escritórios para carimbar a data atual e, às

vezes, o tempo, através de tinta em documentos em papel, para registrar quando o mesmo foi recebido. Um exemplo desse tipo de registro de data e hora é o carimbo em uma carta convencional postada nos correios. Atualmente, o uso desse termo se expandiu, para se referir a informações digitais de data e hora anexadas a dados digitais. Por exemplo, os arquivos de computador contêm registros de data e hora que informam quando o arquivo foi modificado pela última vez. Em termos computacionais, há uma diferença sutil entre um registro de data e hora, obtida pela função datetime(), e o registro obtido por timestamp(), a saber:

a) **Datetime():** contém data e hora civis, sem considerar o fuso horário, ou seja, 08/07/2018 às 10h00min no Brasil é diferente de 08/07/2018 às 10h00min na Itália;
b) **Timestamp():** é um número que determina um momento específico. Tipicamente é expresso como o "número de segundos desde 1/1/1970 às 00h00min em Londres", mas poderia ser qualquer outra base. A ideia do timestamp é que ele vale no mundo todo, independente do fuso horário, ou seja, ele identifica o momento exato em que algo aconteceu. Um evento com timestamp "0" ocorreu em 31/12/1969 às 21h00min no Brasil e em 31/12/1969 às 24h00min em Londres. O timestamp é útil para se registrar logs, e para se verificar se determinado evento “A” aconteceu antes ou depois de determinado evento “B”, independentemente se “A” e “B” tenham acontecido em lados opostos do planeta. Por outro lado, o timestamp é inadequado para registrar datas e horas "civis", porque a hora, e até a data mudam conforme o fuso horário em que o timestamp é interpretado.

Na tecnologia Blockchain, o timestamp é utilizado para se registrar o momento em que um determinado bloco foi criado, independentemente do local onde o fato ocorreu. Este mecanismo será mais bem detalhado na seção 2.2 (Funcionamento do Blockchain).

2.1.5. Carteiras

Carteiras, também conhecidas como Wallets ou eWallets, são softwares que interagem com o usuário gerando suas chaves privadas e públicas e seu endereço (Wallet Address), bem como disponibilizando funcionalidades para administração destas chaves, como: backup, assinaturas, envio de transações, monitoramento de recebimento de transações, *UTXOs* (Unspent Transaction Output ou saídas de transações não gastas, a ser definida na seção 2.2.2), etc. A exploração de vulnerabilidades nas carteiras pode tanto facilitar o roubo de informações, como também revelar a identidade do usuário, trazendo consigo prejuízos irreversíveis. Para mitigar essa possibilidade, surge o Wallet Address (também conhecido

como Blockchain Identity). Como o próprio nome sugere, o Wallet Adress é um identificador único para a Wallet, através da qual somos identificados anonimamente numa rede Blockchain e compartilhada entre os integrantes da mesma, a qual queremos realizar alguma transação. Trata-se, portanto de mais uma camada de segurança para proteção das chaves públicas e privadas do usuário, a qual é obtida da seguinte forma:

a) A Wallet gera randomicamente a chave privada e através do algoritmo ECDSA (abordado no item 2.1.1) gera a chave pública;
b) Obtêm-se o hash da chave pública utilizando o algoritmo SHA-256 (abordado no item 2.1.2);
c) Submete-se o hash obtido no item anterior a um novo hash, utilizando o algoritmo RIPEMD160, resultando como saída, um endereço com 160 (cento e sessenta bits);
d) Submete-se o resultado obtido no item anterior ao algoritmo de transformação Base58Check, obtendo como resultado o Wallet Adress.

As Wallets são, portanto, aplicações voltadas para o usuário final, disponíveis na forma de aplicativos web, desktop, mobile e em hardwares dedicados, onde a simplicidade da sua interface funcional, bem como a segurança, devem ser as palavras de ordem. Segundo o site da Blockchain, existem hoje mais de 30 (trinta) milhões de carteiras operando com bitcoin, através de dezenas de variedades delas (Bitcoin Wallet). Existem várias modalidades de carteiras, onde as mesmas podem ser classificadas pelo seu método de segurança das chaves e/ou na geração das mesmas [Agner, 2018].

2.1.5.1. Método de Segurança das Chaves

São classificações pelas quais as carteiras são tipificadas segundo a sua forma de guarda de suas chaves públicas e privadas, a saber:

a) **Hot Wallets:** são as carteiras mais usadas, normalmente em ambientes conectados à Internet, e que apresentam o menor nível de segurança para o usuário, onde toda vez em que uma nova transação precisa ser assinada, o usuário digita uma senha ou PIN (Personal Indentification Number) para recuperar a chave privada e assinar a transação, fazendo com que a mesma fique exposta, mesmo que por alguns instantes;
b) **Cold Wallets (Cold Storages):** sua característica principal é não ter conexão com a Internet. Também são usadas como carteiras em ambiente totalmente off-line, apenas para assinar transações, e leva-las, de alguma outra forma, ao conhecimento da rede Bitcoin. O ideal para

melhoria da segurança, é que as chaves sejam sempre renovadas quando uma transação for efetivada;

c) **Paper Wallets:** neste tipo de carteira, um tipo de cold storage, as chaves privadas são impressas em papel. A segurança deste tipo de carteira depende do ambiente em que as mesmas foram geradas (um computador sem conexão com a Internet) e a forma com que as mesmas são guardadas. Um método de guarda interessante para este tipo de carteira é o M-de-N, que permite que você tenha um número N de papéis, separados fisicamente em locais seguros, e precisará apenas de M destes papéis, para interagir com a rede Bitcoin. Assim, além da guarda das chaves não estarem em um ambiente conectado, poderá existir a proteção contra um único ponto de falha, já que, caso um papel seja destruído ou roubado, os bitcoins ainda estarão seguros para serem enviados para uma nova carteira segura;

d) **Hardware Wallets:** também considerada um tipo de cold storage. Tecnicamente, este tipo de carteira se vale de dois hardwares, um que assina (dispositivo desconectado da rede) e outro que efetivamente monta e transmite a transação (conectado com a rede). O procedimento então, se sucede da seguinte forma: O usuário, com a carteira conectada, cria uma transação, envia esta transação para ser assinada no hardware Wallet off-line, este então confirma a transação, e logo em seguida tudo que sai do hardware Wallet off-line é a transação assinada, e nada mais, para que o software da carteira conectada possa transmitir esta transação à rede.

2.1.5.2. Método de Geração das Chaves

São classificações pelas quais as carteiras são tipificadas segundo a sua forma de geração de suas chaves públicas e privadas, a saber:

a) **Single-Address Wallets:** são carteiras que utilizam um único endereço para recebimento de transações e trocos, envio etc. Não é um bom tipo de carteira para privacidade e segurança, e por consequência, são cada vez menos utilizadas;

b) **Nondeterministic (Random) Address Wallets:** são carteiras que possuem um armazenamento de tamanho fixo de endereços gerados aleatoriamente. Este modelo traz alguns problemas relativos à segurança dos bitcoins, caso os backups não sejam efetuados regularmente. Neste tipo de carteira, as chaves são geradas e armazenadas de forma aleatória. O usuário não tem como saber quais chaves foram geradas no computador, caso não tenha armazenado as novas chaves no backup. Nessa modalidade, gera-se um conjunto de *n* chaves privadas aleatórias e posteriormente gera-se mais chaves conforme necessário. O backup

desse tipo de carteira é trabalhoso, pois precisa ser mais frequente uma vez que é necessário manter uma cópia de cada nova chave privada;

c) **Deterministic Address Wallets:** são carteiras que geram chaves privadas derivadas, a partir de uma semente (*seed*) em comum. Assim, para a recuperação de seus bitcoins neste tipo de carteira, o usuário só precisa estar de posse de sua *seed* inicialmente gerada. Neste tipo de carteira, diferente das não determinísticas, há a garantia de que todas as chaves privadas serão geradas na mesma ordem, não importando o dispositivo em que ela estiver rodando. Isto facilita a segurança e usabilidade, já que não é mais necessário se repetir o processo de backup da carteira original regularmente, pois somente o backup da semente já é suficiente para recuperar todas as chaves derivadas;

d) **Hierachical Deterministic (HD) Wallets**: são carteiras em que as chaves também são geradas a partir de uma *seed* e todas as demais são geradas em uma ordem não aleatória. A diferença aparece na maneira de gerar suas chaves, formando uma estrutura de árvore, com cada folha na árvore tendo a possibilidade de gerar as chaves filhas e não as acima delas. Isto possibilita uma organização estrutural superior da carteira, com facilidades de organização, divisão de carteiras e, inclusive, a possibilidade de se ter uma carteira dividida por suas folhas, por pessoas de uma empresa, de acordo com a estrutura organizacional, sem comprometer as chaves privadas mestras.

2.1.6. Redes P2P

Trata-se do acrónimo do inglês (Peer-to-Peer) ou do português (Ponto a Ponto). Segundo a Wikipédia, é uma arquitetura de redes de computadores, onde cada um dos pontos, ou nós da rede, funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados, sem a necessidade de um servidor central. Uma rede P2P é mais conveniente para o armazenamento de objetos imutáveis, seu uso em objetos mutáveis é mais desafiador, e pode ser resolvido com a utilização de servidores confiáveis, para gerenciar uma sequência de versões e identificar a versão corrente. Ela pode ser usada para compartilhar músicas, vídeos, imagens, dados, enfim qualquer coisa com formato digital.

Os sistemas cliente-servidor tradicionais, gerenciam e fornecem acesso a recursos como arquivos, páginas Web, ou outros objetos, localizados em um único computador servidor. Nesses projetos centralizados, são exigidas poucas decisões sobre a distribuição dos recursos ou sobre o gerenciamento dos recursos de hardware. Os sistemas P2P fornecem acesso a recursos de informação localizados em computadores de toda a rede. Esse tipo de arquitetura de rede é muito conhecido pelo compartilhamento de arquivos, no entanto, as

redes P2P são utilizadas para outras áreas, tais como armazenamento distribuído em meios acadêmicos e científicos e telecomunicações. São exemplos de redes P2P o Napster, Gnutella e o BitTorrent.

Essa arquitetura depende de alto desempenho da Internet. Como os recursos necessários são distribuídos entre os nós (carga computacional, tráfego de rede, espaço de armazenamento, etc.), é possível conseguir um melhor desempenho de forma econômica, diferentemente da rede cliente-servidor, onde a performance depende do desempenho do servidor. A arquitetura P2P apresenta maior disponibilidade de dados, visto que o objeto pode ser disponibilizado em inúmeros nós da Internet, porém a garantia da segurança é inferior aos outros projetos de compartilhamento de dados.

Segundo [Drescher, 2018], um sistema P2P distribuído que utilize a Internet como meio de comunicação é caracterizado pelos seguintes fatores:

a) Cada computador está conectado ao sistema pela Internet;
b) Cada computador é identificado por um endereço único;
c) Cada computador pode se desconectar e se reconectar ao sistema em qualquer momento;
d) Cada computador mantém, independentemente, uma lista de pares com os quais se comunica;
e) A comunicação entre os nós é baseada em mensagens;
f) As mensagens são enviadas de um nó para outro pela Internet usando seus endereços únicos.

Ainda segundo [Drescher, 2018], em função das adversidades nas redes, a comunicação entre os nós é caracterizada pelos seguintes fatores:

a) Não há garantias de que as mensagens chegarão aos destinatários (elas podem se perder);
b) As mensagens podem chegar mais de uma vez;
c) As mensagens podem chegar numa ordem diferente daquela em que foram enviadas.

A tecnologia Blockchain se defende das adversidades na comunicação em uma rede não confiável da seguinte forma:

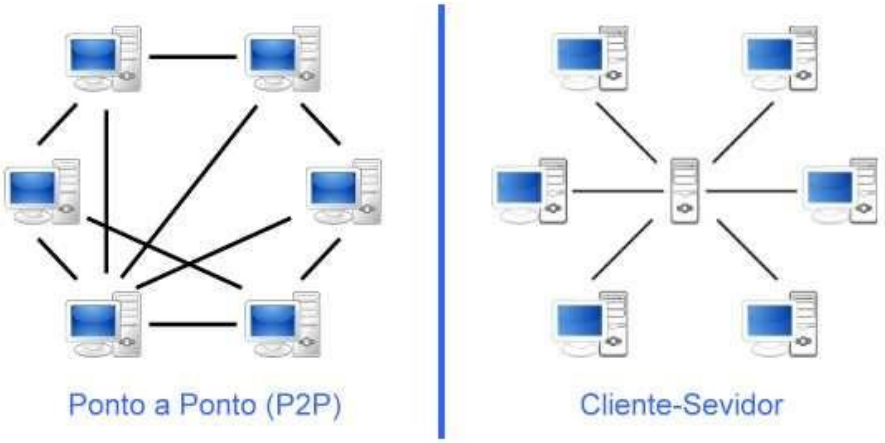
a) As mensagens são enviadas em estilo fofoca (*gossip*). Todo nó que receber uma mensagem a encaminhará aos pares com quem ele se comunica. Esses, por sua vez, tratarão a mensagem do mesmo modo;

b) Duplicatas de transações ou de blocos são identificadas e filtradas com base em seus valores de hash criptográficos (identidades digitais);

c) Todo nó é capaz de ordenar cronologicamente as informações recebidas porque os dados de transação e os cabeçalhos de bloco contém timestamp.

A Figura 2.11, a seguir, apresenta a estrutura dos dois modelos de arquitetura citados.

Figura 2.11 - Arquiteturas P2P e Cliente-Servidor.



Fonte: (Wikpédia).

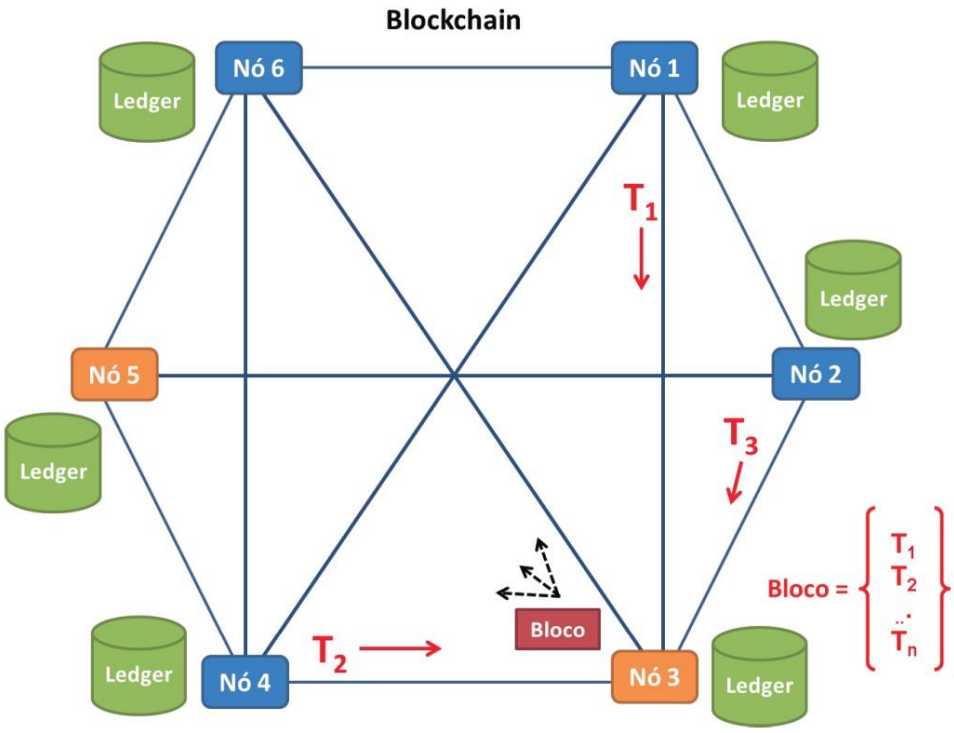
Segundo [Pires, 2016], outra característica importante das redes P2P, especialmente para a utilização com a tecnologia Blockchain, é o seu caráter descentralizado. Informações transmitidas por um nó da rede podem rapidamente ser replicadas para máquinas em diversos lugares do mundo inteiro, tornando praticamente impossível apagar ou alterar registros espalhados em um número tão grande de nós. A forma como as informações são compartilhadas em redes P2P distribuídas, resulta em troca de informações diretamente entre os pares, sem a necessidade de uma entidade central, garantindo a efetividade das transações, onde a confiança reside na rede e não nas pessoas. A seção 2.2 (Funcionamento do Blockchain) apresenta com mais detalhes como os registros do Blockchain são criados, agrupados em blocos, validados por mineradores e espalhados pela rede.

2.2. FUNCIONAMENTO DO BLOCKCHAIN

Esta seção apresenta o mecanismo de funcionamento da tecnologia Blockchain, com base nos conceitos apresentados na seção anterior, tendo como referência o Blockchain do Bitcoin, a implementação de Blockchain atualmente mais popular.

Segundo [Braga, 2017], um Blockchain (corrente de blocos) é uma tecnologia para base de dados distribuída e compartilhada pelos nós de um sistema distribuído, organizado como uma rede P2P. A exemplo do termo contábil “Livro Razão”, que registra todas as transações de uma determinada conta, ele também é conhecido como Ledger ou DLT (*Distributed Ledger Tecnology*). Qualquer nó desta rede, com os direitos de acesso adequados, pode consultar e atualizar a Ledger. Os registros desta base de dados (Ledger) são chamados de blocos, que por sua vez armazenam transações (como um container), que é a sua unidade de informação. A transação pode representar praticamente tudo o que for de valor e importância para a humanidade: dinheiro, ativos financeiros, músicas, propriedades, contratos, certidões, e tudo o mais que possa ser expresso em código. Qualquer nó é livre para colaborar com a rede, propondo novos blocos com transações, tornando-se assim um minerador. Essa base de dados somente aceita a inclusão de blocos novos e nunca a remoção ou modificação de blocos existentes. Por isto, a coleção de blocos é crescente e guarda a história, desde a sua criação até o momento da atualização mais recente. Um Blockchain é um ambiente seguro para registro de transações, uma vez que não há adulteração e nem modificação dos registros já feitos, segurança esta, garantida pelo uso de criptografia e assinaturas digitais. O Blockchain é mantido simultaneamente por todos os nós da rede P2P, não existindo local principal ou preferencial para armazenamento de uma Ledger original. Todo nó tem a sua réplica da Ledger, e todas elas são mantidas íntegras, consistentes e sincronizadas pelos protocolos de consenso (Figura 2.12). Isto significa que todos os nós da rede precisam reconhecer a transação para ela se tornar válida.

Figura 2.12 - Blockchain como uma base de dados distribuída.



Fonte: (Braga, 2017).

O Blockchain então funciona como um banco de dados distribuído que garante a autenticidade e integridade de suas transações, partindo da impossibilidade de qualquer tipo de adulteração das mesmas. O Blockchain é uma tecnologia extremamente revolucionária que permite a desintermediação de transações de valores entre partes que naturalmente não se confiam. Segundo [Tapscott, 2016], o funcionamento do Blockchain é o ápice da colaboração em massa. Você tem domínio sobre seus dados, sua propriedade e seu nível de participação. É a força da computação distribuída permitindo o coletivo disseminado da humanidade. Assim, ele também é conhecido como "o protocolo da confiança". Segundo [Mougayar, 2017], o Blockchain é parte banco de dados, parte plataforma de desenvolvimento, parte viabilizador de rede, então consequentemente, precisamos de muitas instâncias e variações dele. Como uma camada acima da Internet, os Blockchains podem ter muitas formas de implementação. Eles podem ser vistos como camadas de confiança, um mediador de troca, uma conexão segura, um conjunto de capacidades descentralizadas e muito mais. De uma forma resumida, possui as seguintes características básicas:

a) **Transparência:** é possível ter a visualização de qualquer transação, por qualquer nó da rede, disponibilizada em ordem cronológica, salvaguardando a privacidade de seus usuários por

meio de pseudônimos, pois apenas os endereços das transações são mostrados. É uma tecnologia aberta, a qual pode ser avaliada e melhorada por profissionais do mundo inteiro, através de desenvolvimento colaborativo, sendo público o aperfeiçoamento do sistema, onde qualquer programador pode contribuir na sua melhoria. Com a tecnologia open source (código aberto), o Blockchain pode inovar constantemente, interar e melhorar com base no consenso da rede;

b) **Descentralizado:** o sistema distribui poder através de uma rede P2P sem nenhum ponto de controle. Não há centralização das informações, muito menos a necessidade da existência de um ente intermediário que valide as transações. Cada nó da rede possui uma cópia da Ledger. Sem a autoridade central que atua como centro de compensação para a validação de transações, o esforço necessário para alcançar o consenso é compartilhado entre os usuários;

c) **Segurança:** medidas de segurança estão incorporadas na rede sem nenhum ponto de falha, e fornecem não só confidencialidade, mas também autenticidade e aceitação a todas as atividades. O banco de dados é imutável, ou seja, não pode ser alterado, revisado ou adulterado, graças a utilização de criptografia pesada (funções hash usadas na geração de endereços dos blocos, conferindo também sigilo e privacidade dos envolvidos nas transações), assinatura digital (utilizada para garantir a integridade, autenticidade e irrefutabilidade das transações) e alto poder computacional distribuído. Nem os "nós" nem ninguém, exceto o remetente e o destinatário, podem acessar os dados, na sua íntegra, enviados através do Blockchain;

d) **Confiança:** a confiança é a condição essencial da economia digital. A validação de uma transação requer consenso entre os nós da rede. A disponibilidade é geralmente alta porque alguns nós, fora do ar, não impedem o funcionamento dos outros nós, preservando a capacidade de se chegar ao consenso. Cada mecanismo de consenso requer uma quantidade mínima de nós disponíveis (operantes e conectados) para que o mesmo seja viável. Há redundância da Ledger em todos os nós da rede, A tecnologia Blockchain oferece meios confiáveis e eficazes não só de eliminar os intermediários, mas também de reduzir radicalmente os custos das transações envolvidas;

e) **Automatizado:** os softwares envolvidos no processo não permitem que haja duplicidade ou conflito de transações. Transações que não estejam em conformidade com as regras preestabelecidas, não serão registradas no Blockchain.

Assim, o Blockchain é definido como um livro-razão (ledger) digital, distribuído e descentralizado que registra transações através de uma rede global de computadores, onde a

informação é altamente segura. O Blockchain vem sendo definido como sinônimo de transações confiáveis e descentralizadas. As seções a seguir, procuram abordar os pilares de sustentação da tecnologia Blockchain: uso de algoritmos criptográficos (assinaturas digitais e hash), a estrutura de dados, composta de blocos e transações encadeadas, e o mecanismo de consenso utilizado na mineração.

2.2.1. Cadeia de Blocos

Conforme abordado anteriormente, o Blockchain é uma estrutura de dados ordenada, cujos registros são chamados de blocos, encadeados entre si, que por sua vez armazenam transações, que é a sua unidade de informação. Segundo [Agner, 2018], cada bloco é uma estrutura de dados que contém as transações a serem incluídas no Blockchain por meio do trabalho dos mineradores na rede, a ser abordada na seção 2.2.3 (Validação / Mineração). O encadeamento se dá através da ligação entre os blocos, onde cada bloco aponta para um bloco anterior, criando uma corrente desde o bloco inicial até o bloco atual, onde primeiro bloco, também chamado de bloco 0 (zero), é conhecido como bloco gênesis. O bloco gênesis do Bitcoin foi minerado por Satoshi Nakamoto em 1 de setembro de 2009, e é o ponto de partida comum a todas as suas implementações. De uma forma simplificada, no Bitcoin, todo bloco é composto por um cabeçalho e uma lista de transações (Tabela 2.1):

Tabela 2.1 – Estrutura de um Bloco.

Campo	Tamanho	Descrição
Tamanho do Bloco	4 *bytes*	Tamanho do bloco (*block size*) em *bytes* a partir deste campo.
Cabeçalho do Bloco	80 *bytes*	Cabeçalho do bloco (*block header*) contendo metadados.
Contador de Transações	1-9 *bytes*	Número de transações neste bloco.
Transações	Variável	Transações deste bloco.
Hash do Bloco	32 *bytes*	*Hash* do bloco (*hash block*)

Fonte: (Agner, 2018, adaptado).

É através do cabeçalho que se concatena os blocos, cuja estrutura contém os seguintes campos (Tabela 2.2):

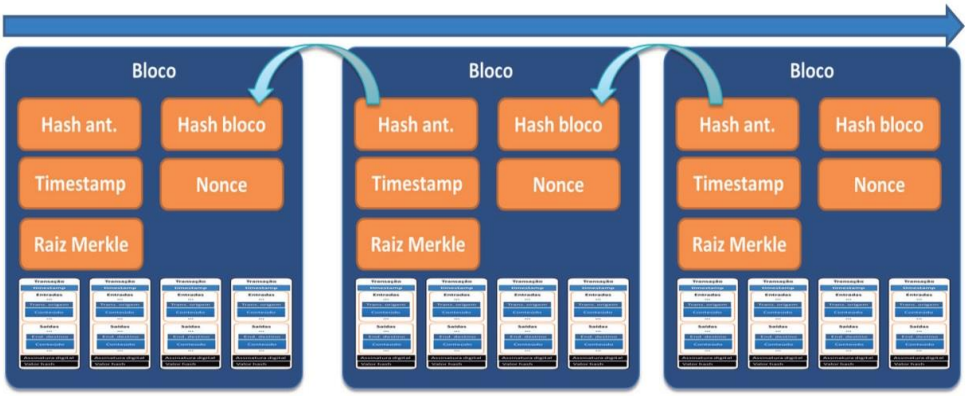
Tabela 2.2 – Estrutura de um cabeçalho de bloco.

Campo	Tamanho	Descrição
Versão	4 *bytes*	Número de versão do bloco. Indica que regras este bloco segue.
Hash do Cabeçalho do Bloco Anterior	32 *bytes*	*Hash* do cabeçalho do bloco anterior (*parent block*) a este na blockchain.
Raiz de Merkle	32 *bytes*	*Hash* da raiz de Merkle das transações deste bloco.
Timestamp	4 *bytes*	Hora aproximada da criação deste bloco. Tempo em segundos no padrão UNIX.
Dificuldade de Alvo	4 *bytes*	Dificuldade de alvo do algoritmo de *proof-of-work (Pow)* para este bloco.
Nonce	4 *bytes*	Contador utilizado como *nonce* no algoritmo de *proof-of-work (Pow).*

Fonte: (Agner, 2018, adaptado).

Como se pode observar na Figura 2.13, o elo entre os blocos se dá através do hash do bloco anterior. Essa característica faz com que o Blockchain seja visto como uma corrente de blocos (origem do nome da tecnologia), com o hash de cada bloco funcionando como elo entre eles. O hash de cada bloco, conforme afirmado acima, é calculado a partir da concatenação dos 6 (seis) campos de seu cabeçalho a saber: versão, hash do bloco anterior, raiz de Merkle, timestamp, dificuldade de alvo e nonce. Registre-se que, o fato da dificuldade de alvo fazer parte do cabeçalho do bloco e, consequentemente, também fazer parte do seu hash, lhe confere a garantia de que ninguém será capaz de evitar os custos de processamento da *Pow*, a ser abordado no item 2.2.3 (Validação / Mineração), reduzindo arbitrariamente a sua dificuldade de alvo.

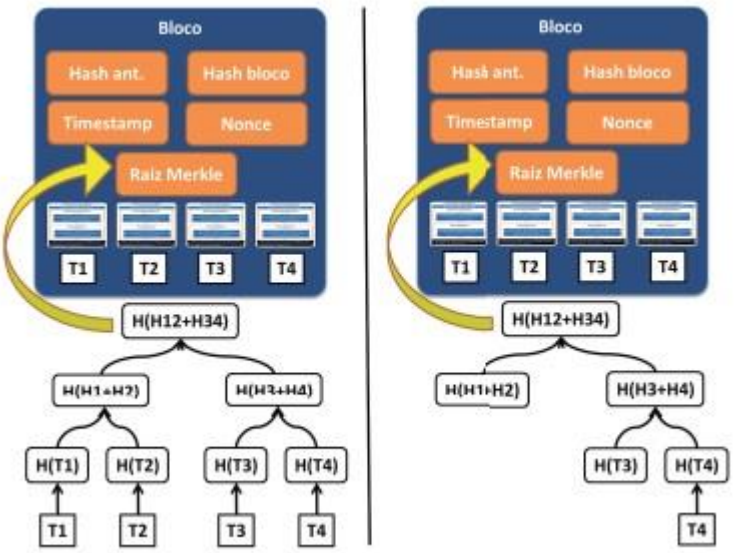
Figura 2.13 - A cadeia de blocos.



Fonte: (Braga, 2017).

Na área de transações, a ser detalhada na próxima seção, estão registradas todas as transações coletadas em cada bloco, onde as mesmas estão sintetizadas no cabeçalho através de sua árvore de Merkle. As transações estão ordenadas entre si de acordo com uma estrutura em árvore binária baseada em hashes, que são os seus endereços únicos. Esse tipo de estrutura facilita a operação de verificação de uma determinada transação num bloco. A Figura 2.14 ilustra a estrutura da árvore de Merkle e a verificação de uma transação no bloco. Na prática essas árvores são bem maiores e proporcionais ao número de transações de cada bloco. Cada hash tem um tamanho de 32 bytes. No exemplo apresentado na Figura 2.14, para comprovarmos que a transação 4 (quatro) está incluída no bloco, precisamos de apenas 3 (três) hashes, totalizando 96 (noventa e seis) bytes para formar o caminho da árvore Merkle.

Figura 2.14 - Árvore Merkle das transações de um bloco.



Fonte: (Braga, 2017).

Na medida em que se aumenta o número de transações, mais evidente fica a eficiência desta estrutura no processo de comprovação da existência de uma determinada transação em um bloco (Tabela 2.3), através do número de bytes do tamanho do caminho de Merkle.

Tabela 2.3 - Eficiência da árvore de Merkle.

Número de Transações	Tamanho Aproximado do Bloco	Tamanho do Caminho de Merkle (*hashes*)	Tamanho do Caminho de Merkle(*bytes*)
4	1 *kilobytes*	3 *hashes*	96 *bytes*
16	4 *kilobytes*	4 *hashes*	128 *bytes*
512	128 *kilobytes*	9 *hashes*	288 *bytes*
2048	512 *kilobytes*	11 *hashes*	352 *bytes*
65.525	16 *megabytes*	16 *hashes*	512 *bytes*

Fonte: (Agner, 2018, adaptado).

O hash de cada bloco possui 2 (duas) funções estruturantes na tecnologia Blockchain: uma de identificador único do bloco e outra, de elo de ligação com o bloco seguinte, onde o mesmo contém um resumo de todas as suas transações. Assim, qualquer alteração no conteúdo de um determinado bloco, implicará necessariamente na alteração de seu hash e por consequência a quebra do elo com o bloco seguinte, além do quê, como veremos adiante, toda transação registrada em um bloco possui uma assinatura digital, o que significa que para se alterar uma transação, necessariamente teríamos que conhecer a chave privada de quem a originou. Mesmo que esta alteração fosse possível, ainda assim, toda cadeia de blocos teria que ser validada e aceita por todos os nós da rede P2P, o que demandaria um esforço computacional enorme, conforme já abordado na seção 2.2 (Funcionamento do Blockchain). Isto confere ao Blockchain uma imutabilidade que cresce exponencialmente a cada novo bloco inserido na cadeia.

2.2.2. Transações

A transação, no Bitcoin, nada mais é do que a estrutura de dados responsável pela transferência de valor de um ou mais inputs (fonte de fundos) para um ou mais outputs (destino dos fundos). A exemplo dos blocos, descritos na seção anterior, as transações também são encadeadas. De uma forma simplificada, a estrutura de uma transação, no Bitcoin, é constituída da seguinte forma (Tabela 2.4):

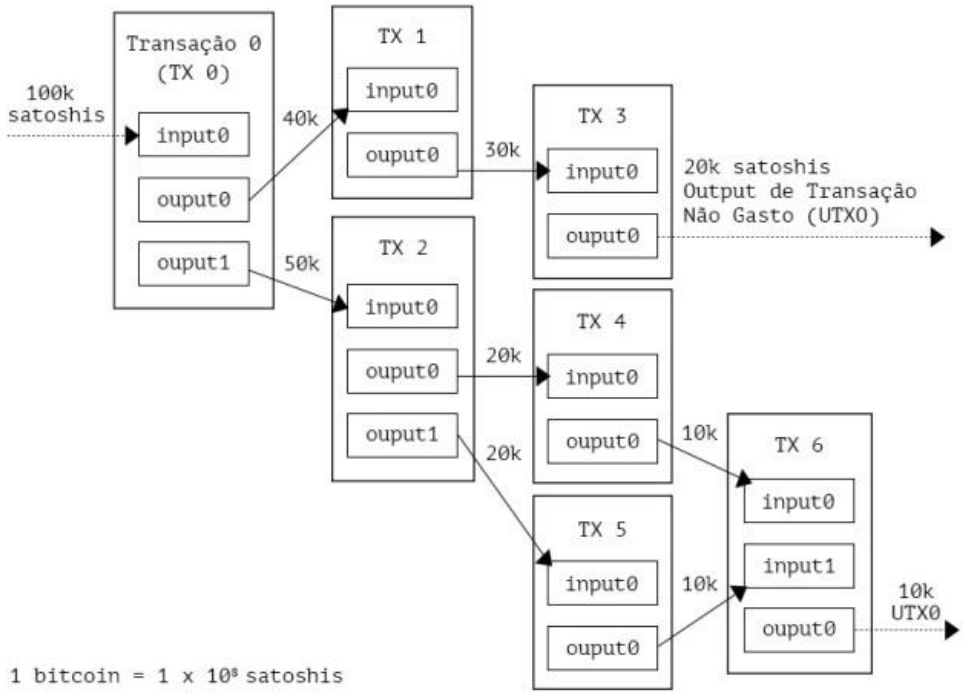
Tabela 2.4 – Estrutura de uma transação.

Campo	Descrição	Tamanho
version	Identifica as regras que a transação segue.	4 *bytes*
tx_in count	Identifica quantos *inputs* a transação tem.	1-9 *bytes*
tx_in	O(s) *input(s)* da transação.	Tamanho variável
tx_out count	Identifica quantos *outputs* a transação tem.	1-9 *bytes*
tx_out	O(s) *output(s)* da transação.	Tamanho variável
lock_time	Um *timestamp UNIX* ou um número de bloco a partir de quando/qual a transação poderá ser destrancada.	4 *bytes*

Fonte: (Agner, 2018).

As transações são encadeadas através dos seus inputs e outputs, ou seja, o output de uma transação aponta para o input de uma transação seguinte (Figura 2.15). Os outputs prontos para serem usados em uma nova transação são chamados de *UTXO* (Unspent Transaction Output ou saída de transações não gastas).

Figura 2.15 - Encadeamento de transações no Blockchain.



Fonte: (Agner, 2018).

De uma forma simplificada, a estrutura de um output é constituída dos seguintes campos (Tabela 2.5):

Tabela 2.5 – Estrutura de um output de uma transação.

Campo	Descrição	Tamanho
value	Número de *satoshis* (BTC/10^8) a serem transferidos .	8 *bytes*
locking-script length	O tamanho do *locking script* em *bytes*.	1-9 *bytes*
locking-script	Um *script* com as condições necessárias para o *output* ser gasto.	Tamanho variável

Fonte: (Agner, 2018).

O *locking-script* é uma espécie de condição de destravamento para o recurso (output) ser utilizado. Da mesma forma, a estrutura de um input é constituída dos seguintes campos (Tabela 2.6):

Tabela 2.6 - Estrutura de um input de uma transação.

Campo	Descrição	Tamanho
tx Hash	Identificador da transação que contém os *UTXOs* a serem gastos .	32 *bytes*
output index	Índice do *UTXO* a da transação a ser gasto.	4 *bytes*
Unlocking script length	Tamanho do *unlocking-script* em *bytes*.	1-9 bytes
Unlocking script	O *unlocking-script* que responde as condições do *locking script* do *UTXO* a ser gasto.	Tamanho variável
*sequence number	Sequência para ser usada por *feature* de substituição de transação (atualmente, não utilizado).	4 *bytes*

Fonte: (Agner, 2018).

O *unlocking-script* é, portanto, o atendimento à condição estabelecida no seu *locking-script* correspondente, é aqui que entra a assinatura do usuário.

Assim, enviar Bitcoins consiste basicamente em assinar digitalmente um conjunto de dados compostos pela quantia, um ponteiro para a transação anterior, o destinatário do valor, dentre outros. Como se pode verificar, a estrutura dos dados de uma transação é composta de campos, cujos conteúdos são definidos ao longo do seu ciclo de vida, ou seja, durante um processo que se inicia com a sua criação até a sua inclusão e posterior validação num Blockchain por um minerador (melhor detalhada na próxima seção). Assim, uma transação só será bem sucedida após o seu ciclo se findar com êxito. Podemos definir uma transação como um segmento assinado de dados que é transmitido pela rede e que, quando devidamente validado, passa a fazer parte de um bloco, que por sua vez quando obtido o consenso de um dos nós da rede, é incluído na cadeia de blocos do Blockchain. Assim, podemos afirmar que as transações são a parte mais importante de qualquer Blockchain. De uma forma

simplificada, podemos resumir o ciclo de vida de uma transação, envolvendo a transferência de recursos entre 2 (dois) usuários, em 4 (quatro) etapas, a saber:

a) **Preparação das partes envolvidas:** geração e divulgação do endereço (Wallet Adress) do creditado para o debitado;

b) **Registro da transação:** criação, assinatura e propagação da transação entre os nós da rede, pelo debitado;

c) **Consenso:** os nós da rede recebem a transação e passam a trabalhar na busca do consenso (mineração), quando um determinado nó valida a transação, a mesma é então incluída num bloco e é propagada na rede para ser aceita, quando então o bloco passa a fazer parte do Blockchain, e;

d) **Consulta ou confirmação:** o creditado consulta a Ledger e entende que sua transação foi aceita.

A Figura 2.16, ilustra o fluxo completo de ações para a realização de uma transação Blockchain, envolvendo dois usuários: Alice e Bob, onde Bob transfere algum recurso para Alice, a saber:

a) **Preparação das partes envolvidas:**

1. Alice cria sua conta (gera/escolhe um endereço que é a sua própria Wallet Adress);
2. Alice divulga sua conta (Wallet Adress) para Bob.

b) **Registro da transação:**

3. Bob forma uma transação (Wallet Adress/chave pública de Bob, valor a ser transferido, data e hora da transação e Wallet Adress/chave pública de Alice) e a assina digitalmente;
4. Bob propaga a transação entre os nós da rede P2P, neste momento, tanto Bob como Alice enxergam a transação na rede como "não confirmada".

c) **Consenso:**

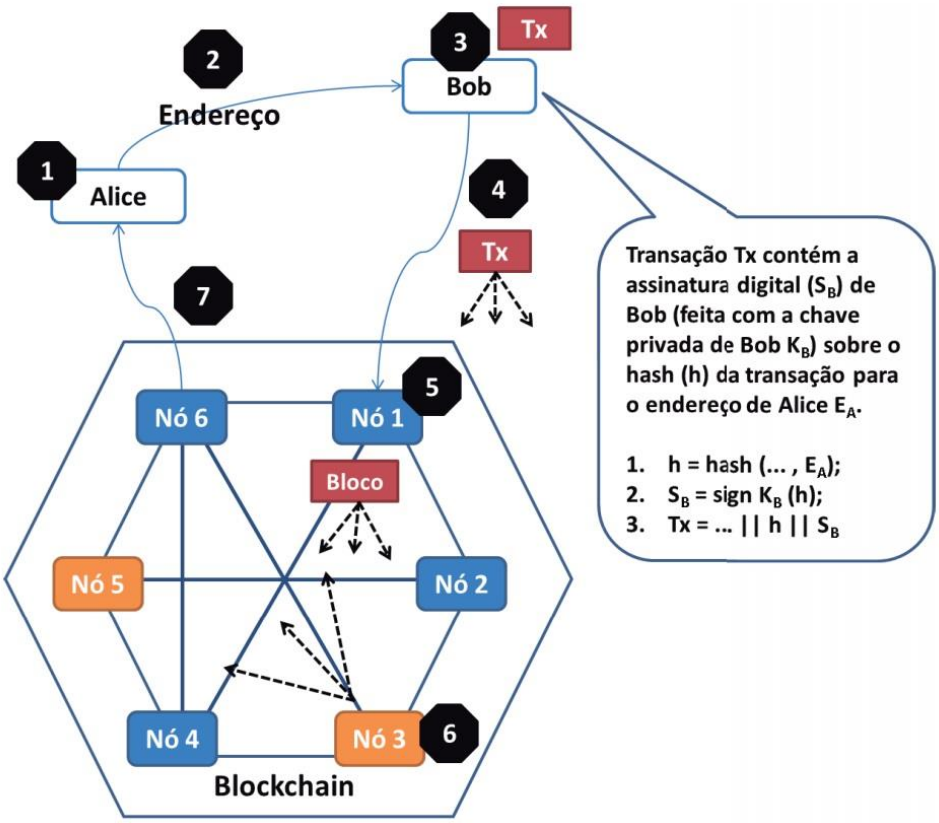
5. Os nós da rede trabalham para obter o consenso e a transação é incluída em um bloco, de acordo com as regras da transação;
6. Os nós da rede P2P propagam seu resultado para outros nós, a transação é aceita de acordo com o consenso e passa a fazer parte do Blockchain.

d) **Consulta ou confirmação:**

7. Alice consulta a Ledger e entende que sua transação foi aceita.

Segundo [Braga, 2017], muitas vezes, devido à natureza assíncrona da comunicação e ao tempo relativamente longo (para máquinas e não para pessoas) necessário para a realização do consenso, o último passo (confirmação) não é realizado, gerando com isto, uma vulnerabilidade ao processo.

Figura 2.16 - Fluxo de ações numa transação Blockchain.



Fonte: (Braga, 2017).

2.2.3. Validação / Mineração

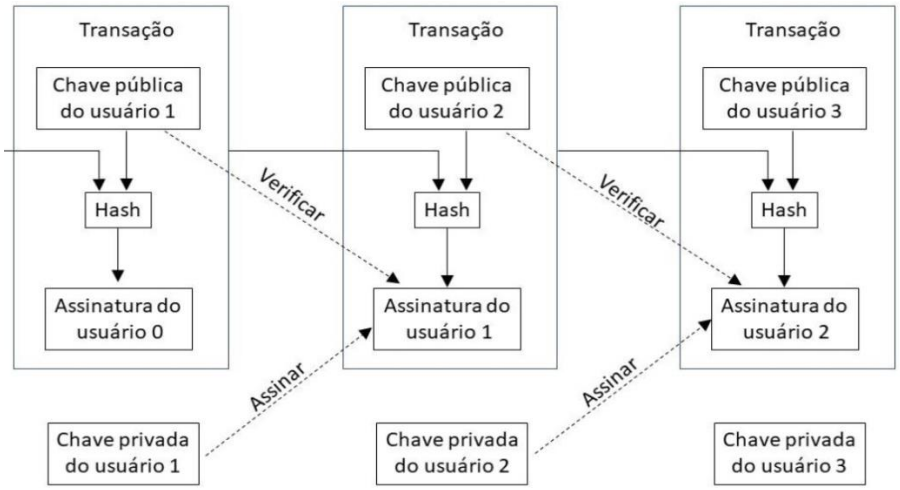
Conforme citado anteriormente, quando uma transação é gerada, a mesma é propagada entre os nós da rede, os quais passam a trabalhar na formação de um bloco de consenso (mineração) entre os mesmos. Os participantes concordam que quem resolver o problema primeiro pode criar o próximo bloco. A mineração, portanto, é o conjunto de ações, na busca da validação da transação propagada, através da montagem de um bloco, que ao ser devidamente checado pelos nós da rede, culmina na sua inclusão no Blockchain, ou no seu descarte.

Os mineradores recebem constantemente as transações geradas pelos usuários, e, portanto ainda não confirmadas, e as armazenam temporariamente em uma estrutura em memória chamada *"mempool"*, quando então realizam uma minuciosa análise de consistência das transações através de alguns procedimentos de controle. Esses procedimentos incluem regras de correção formal, semântica e autorização, a saber:

a) **Verificação da formatação da transação:** conferência e validação das informações quanto ao seu preenchimento e formatos**;**

b) **Verificação das assinaturas envolvidas:** consiste em verificar se o usuário que está transferindo o recurso referente a transação é, de fato, o usuário que deveria estar transferindo o recurso (checagem das assinaturas e endereços envolvidos). A chave pública informada no campo entrada da transação é comparada com a chave pública previamente inserida na saída da mesma. Caso elas sejam diferentes, a transação é considerada inválida e não é propagada para os demais nós da rede. Caso elas sejam iguais, a assinatura informada no campo entrada é verificada com a chave pública previamente confirmada. Se a assinatura for autêntica, ou seja, se a decriptação com a chave pública revelar o hash dos dados da transação, então a transação é validada (Figura 2.17);

Figura 2.17 - Processo de validação de transação.



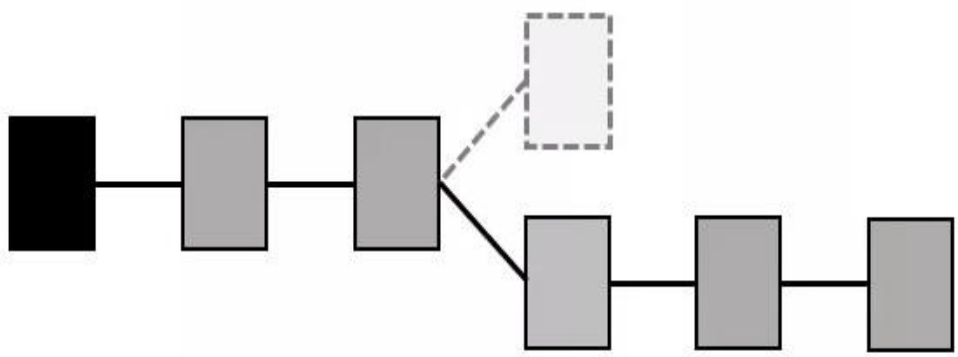
Fonte: (Nakamoto, 2009).

c) **Verificação do gasto duplo:** consiste em verificar se o usuário que está transferindo o recurso possui saldo suficiente para efetuar a transação (evitar gasto duplicado). Caso um usuário tente realizar duas transações simultâneas, caracterizando um gasto duplo, haveria 2 (duas) situações, a saber:

1. As 2 (duas) transações são recepcionadas por um mesmo minerador. Nesta situação, apenas a primeira transação recepcionada será aproveitada;

2. As 2 (duas) transações são recepcionadas por mineradores distintos. Nesta situação, cada minerador utilizará a transação recepcionada na formação de seu bloco. A solução, para este caso, só virá quando um terceiro minerador encontrar um novo bloco e escolher, arbitrariamente, uma das vias da bifurcação para ser estendida. Uma vez que uma das vias foi estendida, essa via será considerada a maior cadeia de blocos, e outros nós trabalharão para estendê-la, abandonando a outra via menor e, consequentemente, resolvendo o gasto em duplicidade (Figura 2.18). Este procedimento é chamado de Regra da Maior Cadeia (*Longest Chain Rule*) e baseia-se na ideia de que a estrutura de dados Blockchain contendo o maior número de blocos representa o máximo de esforço computacional agregado, onde a escolha da extensão da cadeia, quando da ocorrência de uma bifurcação, é feita em função da somatória da "Dificuldade de Alvo", definido na seção 2.2.1 (Cadeia de Blocos) de todos os blocos que pertencem ao caminho a ser escolhido (Regra da Cadeia Mais Pesada).

Figura 2.18 - Regra da maior cadeia.



Fonte: (Martins, 2018).

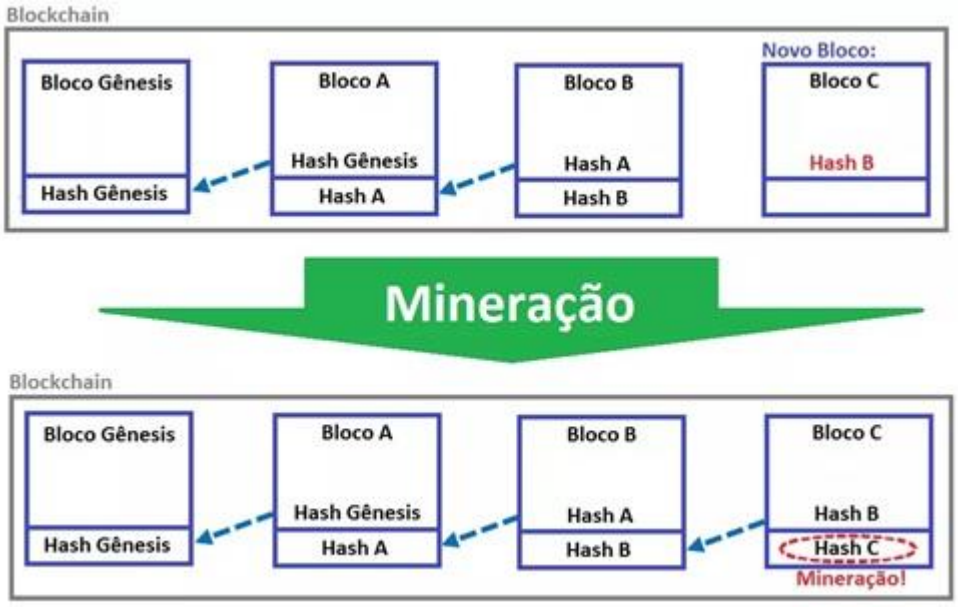
Na sequência, caso haja alguma inconsistência neste processo, o minerador descarta a transação proposta, caso contrário, ou seja, se tudo estiver consistente, o minerador então agrega as transações em um bloco a ser minerado, calcula a sua raiz de merkle, em função das transações agregadas, e então parte para a busca de um nonce específico, visando o cálculo do hash do bloco, conforme as regras estabelecidas no mesmo. O nonce, conforme definido na seção 2.2.1 (Cadeia de Blocos), é um campo de 32 bits (4 bytes) cujo valor é ajustado pelos mineradores, de tal maneira que o hash do bloco que está sendo minerado, seja menor ou igual à dificuldade de alvo, campo de 32 bits (4 bytes), também definida no próprio bloco. Assim, o hash de um bloco é estabelecido quando se encontra o nonce que satisfaça essas

regras, portanto, a mineração nada mais é do que o processo de se encontrar o nonce válido. Uma vez estabelecido esse hash, qualquer alteração nos dados do bloco, como se sabe, fará com que o hash do bloco seja completamente diferente. Como é inviável se prever qual combinação de bits resultará no hash, muitos valores diferentes de nonce são tentados, e o hash é recalculado para cada valor de nonce, até que a dificuldade de alvo estabelecida seja atendida. A este cálculo iterativo, que requer tempo e recursos computacionais adequados, chamamos de prova de trabalho (*Proof of Work ou PoW*). A dificuldade do *Proof of Work* é obtida pela definição dos "n" bits mais à esquerda do hash do bloco processado, que precisam ser iguais à zero. Tipicamente, uma prova de trabalho é um processo probabilístico, e a probabilidade de seu sucesso depende da dificuldade de alvo estabelecida. Quanto menor a dificuldade de alvo (mais zeros à esquerda), menor a probabilidade de sucesso e mais difícil se torna a prova de trabalho. Assim, a probabilidade de um nó "encontrar o próximo bloco" é proporcional ao seu poder computacional dentro da rede. O protocolo do Bitcoin ajusta a dificuldade de alvo automaticamente a cada 2016 blocos (~ 2 semanas) para garantir que a mineração de um bloco aconteça, em média, a cada 10 minutos. Outros Blockchains ajustam esse parâmetro para que a mineração aconteça em intervalos menores, de alguns segundos por exemplo. Quando a prova de trabalho é vencida, o nó avisa toda rede que resolveu o desafio (*broadcasting*) e insere o bloco validado na cadeia de blocos. Ao realizar esta operação, o minerador recebe como recompensa uma quantia na unidade de valor utilizada pelo Blockchain, operação esta conhecida como *coinbase transaction*, criada pelo próprio minerador e atribuída a um endereço de sua escolha. Essa recompensa, portanto, representa a emissão de novas unidades de moeda na rede. Quando o Bitcoin foi criado, em 2009, essa recompensa era de 50 unidades de bitcoin por bloco criado. Atualmente, para cada novo bloco inserido no Blockchain, o minerador ganha 12,5 unidades de bitcoin, e por definição do protocolo, esse valor diminui pela metade a cada 210.000 blocos criados (cerca de 4 anos) e a previsão é a de que até o ano de 2140, se atinja o limite máximo de unidades de bitcoin em circulação que será de 21.000.000 (vinte e um milhões) [Pires, 2016]. Outra forma de recompensa é por meio das taxas de transação cobradas pelos mineradores para incluir uma transação em seu bloco. Ela é usada para definir prioridades entre as transações e evitar *spam*. O autor de uma transação, ao informar o valor total de entrada maior que o valor total de saída, está dando a diferença como taxa para o minerador que incluir aquela transação em seu bloco. O autor da transação pode escolher pagar uma taxa de valor zero, porém corre o risco de ter sua transação ignorada pelos mineradores. Historicamente, essa taxa não era requerida, mas hoje quase todos mineradores esperam receber taxas e no futuro, quando a recompensa

por encontrar blocos for reduzida a zero, as taxas de transação serão o principal meio de recompensa para os mineradores [Rodrigues, 2016].

Como já comentado, todos os nós da rede possuem uma cópia idêntica da Blockchain, formando a chamada *Distributed Ledger* (livro/registro contábil distribuído). Assim, quando um novo bloco é criado por um deles, todos os nós deverão verificar se o bloco é válido. Nesse processo de validação, quando um bloco é validado, ele é imediatamente publicado na rede para todos os nós adjacentes por meio de uma rede P2P. Cada um destes nós recebe o novo bloco, verifica se de fato se trata de um bloco ainda não recebido (cada bloco tem a sua numeração incremental, também chamada de altura do bloco) adiciona o bloco à sua cópia do Blockchain e replica, por sua vez, aos nós adjacentes. Esse ato de aceitação é chamado de confirmação e normalmente usa-se a heurística de pelo menos 6 (seis) confirmações para considerar que um bloco efetivamente faz parte do Blockchain (Figura 2.19). Esse processo se repete por toda a rede, a fim de que haja consenso entre os seus nós, quanto ao estado da cadeia de blocos [Martins, 2018]. Quanto mais poder computacional dedicado à construção do Blockchain, maior será sua resiliência a ataques, principalmente a dados armazenados em blocos mais antigos. Por esse motivo, todos os nós da rede consideram apenas a cadeia com maior trabalho agregado à sua construção, como válida.

Figura 2.19 - Mineração no Blockchain.



Fonte: (Martins, 2018).

Na rede Blockchain do Bitcoin, quando um novo nó é adicionado, é enviada uma mensagem a um ou mais nós específicos gravados no código do programa, chamados de nós

sementes (*seed nodes*), requisitando outros nós da rede, endereços de nós com os quais se possa conectar. Este processo se repete com os nós recém-aprendidos, até que o nó adicionado esteja conectado à vários outros nós da rede de maneira razoavelmente aleatória. Uma vez conectado à rede e com os registros do Blockchain atualizados, o nó está apto a publicar novos registros através de um algoritmo de broadcasting (*flooding* ou *gossip protocol*). De maneira simplificada, o nó envia o registro recém-criado a todos os nós com o qual está conectado. Ao receber um novo registro, cada nó verifica se se trata de um registro novo ou se já o recebeu anteriormente. Caso seja um novo registro, o nó adiciona o registro à sua lista e o replica para todos os nós a ele conectado. Caso o registro já tenha sido recebido anteriormente, ele simplesmente o ignora. Isto impede que mensagens fiquem trafegando indefinidamente pela rede [Pires, 2016].

O *Pow* tem sido amplamente bem sucedido devido as seguintes propriedades:

- É difícil encontrar uma solução para este problema;
- Quando encontrada a solução, é fácil verificar se está correta.

Além do método utilizado pelo protocolo Bitcoin, comentado acima, existem ainda vários outros métodos de consenso utilizados na tecnologia Blockchain, como por exemplo, o Delegated Byzantine Fault Tolerance (DBFT) ou consenso bizantino (caracterizado pela necessidade de 3*n+1 nós na rede P2P para tolerar n divergências no consenso) e a Prova de Participação ou Proof of Stake *(PoS*) utilizada pelo *Ethereum* (uma variação da plataforma Blockchain), fundamentado no conceito de mineração virtual e voto baseado em token, onde os mineradores concorrem para validação dos blocos com o quanto de *Ether* (criptomoeda utilizada pelo *Ethereum*) possuem, um processo que não demanda o mesmo volume de processamento da *PoW*.

Segundo [Drescher, 2018], em qualquer instante, todos os nós do sistema estarão em uma das seguintes situações:

- Avaliando um novo bloco criado por outro nó;
- Esforçando-se para ser o próximo nó a criar um novo bloco que deverá ser avaliado por todos os demais.

Concluindo, o procedimento que governa como os nós lidam com novos dados de transação e novos blocos recebidos de seus pares, pode então ser resumido da seguinte forma:

- Novos dados de transação, assim como novos blocos, são encaminhados a todos os nós, no estilo fofoca (*gossip*);

- Cada nó coleta os novos dados de transação em uma caixa de entrada (*mempool*) e os seleciona para processamento;

- Cada nó processa os novos blocos imediatamente com a mais alta prioridade;

- Cada nó processa os novos dados de transação validando-os quanto à correção formal, semântica e autorização;

- Cada nó reúne somente os dados de transação válidos em uma árvore de Merkle e começa a criar um novo bloco resolvendo o seu *PoW*;

- Assim que um nó termina o seu *PoW*, ele enviará o bloco recém-criado a todos os outros nós;

- Cada nó processa novos blocos verificando a solução de seu *PoW* e conferindo todos os dados de transação contidos no que concerne à correção formal, semântica e autorização;

- Cada nó adiciona os blocos válidos à própria cópia da estrutura de dados Blockchain;

- Se um bloco que acabou de chegar for identificado como inválido, ele será descartado e os nós continuarão processando dados de transação ou terminarão o seu *PoW* de um novo bloco;

- Se um bloco que acabou de chegar for identificado como válido, o nó removerá as transações contidas no novo bloco da própria *mempool* e iniciará o processamento dos dados de transação e a criação de um novo bloco;

- Se um bloco adicionado à estrutura de dados do Blockchain for identificado como inválido ou inútil mais tarde, esse bloco, assim como todos os seus blocos subsequentes, será removido da estrutura de dados do Blockchain e suas transações serão adicionadas na *mempool* para que sejam processadas novamente;

- O nó cujo bloco foi aceito receberá as taxas por todas as transações contidas no bloco como recompensa;

- Se um bloco for removido da estrutura de dados Blockchain, a recompensa por adicioná-lo será retirada do nó que inicialmente a havia recebido.

Como podemos constatar então, criar blocos válidos custa energia, tempo e dinheiro, pois exige resolver a *PoW* para cada bloco, o que é custoso do ponto de vista de processamento. Segundo [Mougayar, 2017], um forte competidor para a *PoW* será o algoritmo de Prova de Participação (*PoS*), que depende do conceito de mineração virtual e voto baseado

em token. O *Pos* elimina o requisito de energia e poder computacional do *Pow* e o substitui por participação. Com o *Pos*, não temos mineradores, e sim validadores.

2.3. CONTRATOS INTELIGENTES

Desde a criação da tecnologia Blockchain, vários especialistas observaram que as suas propriedades intrínsecas, tais como segurança, resiliência, inviolabilidade e imutabilidade, poderiam ser usadas em vários outros tipos de aplicações. Com isso, as plataformas de desenvolvimento Blockchain evoluíram e permitiram a inserção de transações mais complexas, através dos denominados contratos inteligentes (*smart contracts*). Assim, a partir de 2013, surgiu uma nova geração da tecnologia, denominada Blockchain 2.0, onde, além da transação normal definida originalmente no Bitcoin, cada nó também pode armazenar contratos. Segundo [Mougayar, 2017], os contratos inteligentes prometem programar nosso mundo nos Blockchains, e potencialmente substituir alguma das funções atualmente executadas por intermediários lentos ou caros. Estamos falando de programas de computador, replicados e executados por todos os nós da rede, ou por um conjunto predeterminado de nós, denominados validadores. Aplicações baseadas em contratos inteligentes são chamadas *Decentralized Applications* (*Dapps*). A plataforma Ethereum, é um exemplo dessa evolução, e foi proposta no final de 2013 por Vitalik Buterin, um pesquisador e programador de criptomoedas. Ela se baseia em máquinas virtuais descentralizadas denominadas *Ethereum Virtual Machines* (*EVM*), que executam contratos, usando uma criptomoeda denominada *Ether*, através de uma linguagem de programação específica chamada *Solidity*. O uso de recursos como *Dapps* e de contratos inteligentes, permite o desenvolvimento de diferentes tipos de aplicação da tecnologia, não só para o setor financeiro (dinheiro, ações, investimentos, crowdfunding, títulos e derivados), mas também para registros públicos (imóveis, terrenos, registro de veículos, licença comercial, passaporte, identidade, RG, CPF), registros privados (contratos, assinaturas, testamentos, obrigações, garantias), chaves físicas (acesso a casa, hotéis, aluguel de carros, chave de carros), intangíveis (patentes, marcas, reservas, nome de domínios, apostas), etc. Tais características aumentou o interesse de grandes empresas pela plataforma.

Há grandes diferenças entre o Bitcoin e o *Ethereum* a saber:

- No *Ethereum* suas transações duram em média 15 segundos, no Bitcoin ~10 minutos;
- No *Ethereum* o modelo de recompensa na criação de novos blocos, libera a mesma quantidade de *Ether* a cada ano, no Bitcoin a recompensa diminui pela metade a cada 4 anos;

- O *Ethereum* tem seu próprio código interno completo de *Turing*;

- O *Ethereum* foi financiado pela comunidade internacional, o Bitcoin foi lançado, e os seus primeiros mineiros possuem a maioria das moedas que são minadas;

- O *Ethereum*, implementa o conceito de contratos inteligentes, além de transações normais, como o Bitcoin, que são programas de computador que podem ser corretamente executados por uma rede de nós mutuamente suspeitos de uma rede P2P, sem que seja necessária uma entidade externa confiável para mediação do acordo. Os nós da rede são ditos mutuamente suspeitos por que eles não precisam confiar incondicionalmente uns nos outros, uma vez que podem ser competidores ou até mesmo adversários [Braga, 2017].

Segundo [Mougayar, 2017], os contratos inteligentes carregam consigo algumas características, a saber:

a) **Contratos inteligentes não são a mesma coisa que acordos contratuais:** eles farão com que a quebra de um acordo seja cara, pois controlam uma propriedade do mundo real por meios digitais. Eles podem provar se certas condições foram cumpridas ou não, por exemplo, se o pagamento de um carro não for feito no prazo, o veículo fica bloqueado (sem funcionar) até o seu pagamento;
b) **Contratos inteligentes não são como contratos Ricardianos:** considerada uma nova geração dos contratos inteligentes, um contrato Ricardiano é um contrato que contempla duas partes destinadas a dois propósitos: Primeiramente, é um contrato legal e fácil de ler entre duas ou mais partes, onde tanto um advogado, quanto você pode entendê-lo facilmente. Em segundo lugar, é um contrato legível por máquina. Com as plataformas blockchain, esses contratos agora podem ser facilmente criptografados, assinados e salvos na blockchain;
c) **Contratos inteligentes não são a lei:** ainda não existe um marco legal que ampare esta tecnologia. Sendo programas de computador, são apenas tecnologias capacitadoras. Um resultado de um contrato inteligente poderia ser utilizado como rastro auditável para provar se os termos de um acordo legal foram cumpridos ou não;
d) **Contratos inteligentes não incluem inteligência artificial:** são códigos que representam a lógica de negócios que ocorrem em um Blockchain, e como tal, são iniciados por dados externos que permitem a modificação de outros dados;
e) **Contratos inteligentes não são a mesma coisa que aplicações Blockchain:** eles geralmente são parte de uma aplicação descentralizada. Por exemplo, se certas condições em um contrato são respeitadas, então o programa pode atualizar uma base de dados;

f) **Contratos inteligentes são fáceis de ser programados:** as linguagens específicas para contratos inteligentes, como por exemplo, a *Etherium's Solidity*, permite escrever processos complexos em algumas linhas de código. Mas há implementação de contratos inteligentes que usam "oráculos", que são fontes de dados externos que enviam informações para contratos inteligentes, como por exemplo, identidades, endereços, certificados, índices de reajustes, temperaturas etc.;

g) **Contratos inteligentes não são apenas para desenvolvedores:** a próxima geração de Blockchain incluirá facilidades para o usuário na formatação de um contrato inteligente, como interfaces gráficas ou talvez uma linguagem baseada em texto;

h) **Contratos inteligentes são seguros:** eles são programas quasi-Turing completos. Isto significa que há um final em sua execução, e, portanto, não ficam em looping eterno;

i) **Contratos inteligentes possuem uma grande variedade de aplicações:** são programas de computador que protegem, fazem cumprir e executam a liquidação de acordos registrados entre pessoas e organizações. Eles não se limitam a movimentos monetários. Aplicam-se a quase tudo o que muda de estado com o tempo e que pode ter um valor.

Segundo [Tapscott, 2016], a um custo muito baixo, contratos inteligentes permitem às companhias criar acordos engenhosos e auto executáveis com novas classes de fornecedores e parceiros antes improváveis. Quando agregados, contratos inteligentes podem fazer as empresas parecerem redes, tornando as fronteiras corporativas mais permeáveis e fluidas.

2.4. VARIAÇÕES DE BLOCKCHAIN

Como já mencionado, a tecnologia Blockchain visa a descentralização como medida de segurança. Sua base de dados é distribuída e compartilhada, funciona como um livro-razão público e universal, que cria consenso e confiança na comunicação direta entre duas partes, ou seja, sem o intermédio de terceiros. Segundo [Drescher, 2018], a tecnologia Blockchain enfrenta 2 (dois) conflitos, a saber:

a) **Transparência x Privacidade:** ser aberto e transparente é um dos pilares de sustentação da tecnologia Blockchain. É através dessa característica que os seus usuários podem auditar as transações da cadeia. Essa característica, entretanto, se opõe ao conceito de privacidade. Assim, o conflito está entre preservar a transparência necessária para os dados e os requisitos de mais privacidade para seus usuários. Este conflito pode ser associado à operação de leitura da estrutura de dados do Blockchain;

b) **Segurança x Velocidade:** o histórico de dados das transações, armazenados em blocos encadeados, constitui-se no coração da tecnologia Blockchain. Essa estrutura de blocos e seu encadeamento vem revestido de componentes de segurança que conferem à mesma um alto grau de imutabilidade de seus dados. Por um outro lado, essa característica tem um custo: redução da velocidade de processamento de novos dados. Assim, o conflito está entre proteger o histórico de dados das transações, com base na *PoW* que consome tempo, e os requisitos de velocidade e de escalabilidade exigidos por muitas aplicações. Este conflito pode ser associado à operação de escrita na estrutura de dados do Blockchain.

Já existem algumas variantes desta tecnologia (*Side Chains*) quanto a quem é permitido participar na rede, executar o protocolo de consenso e manter a cadeia compartilhada. Cada tipo de Blockchain tem suas vantagens e desvantagens, permitindo-lhes atender às necessidades de várias aplicações:

2.4.1. Pública

Qualquer pessoa pode acessar o sistema, enviar transações ou participar do processo de consenso, este tipo de Blockchain não requer "permissão". Todas as transações são públicas e os usuários podem permanecer anônimos. Como os usuários não se conhecem, o nível de confiança entre eles é baixo, necessitando de uma sobrecarga computacional maior no seu consenso. Assim, a verificação ou validação de cada transação é bastante alta e demorada. O Blockchain do Bitcoin e *Etherium* são exemplos mais conhecido desta variação;

2.4.2. Privada

Os blocos são controlados por uma única organização que determina quem pode ler e enviar transações e participar do processo de consenso. Nesta modalidade, a confiança é maior, pois é baseada na permissão de acesso, e é possível fazer uso de algoritmos compartilhados mais simples e rápidos. Como resultado, em vez de algumas transações por segundo, é possível fazer milhares delas. O *Hyperledger Fabric* é um exemplo de uma implementação de Blockchain privada;

2.4.3. Semiprivada

Os blocos são executados por uma única empresa, que concede acesso a qualquer pessoa que preencha os critérios preestabelecidos. Suas aplicações podem ser especialmente

interessantes para usuários de B2B (*business to business*), por exemplo. O *Ripple* é um exemplo de uma implementação de Blockchain semiprivada;

2.4.4. Consórcio

O processo de consenso é controlado por um grupo pré-selecionado de corporações, mas o direito de ler a cadeia e realizar transações pode ser público ou restrito aos participantes. Os consórcios de Blockchain são considerados "com permissão" e são os mais indicados para a maioria das empresas. As cadeias de bloco do consórcio são principalmente usadas no setor bancário. O processo de consenso é controlado por um conjunto pré-selecionado de nós; por exemplo, pode-se imaginar um consórcio de 15 (quinze) instituições financeiras, cada uma das quais operando um nó e das quais 10 (dez) devem assinar todos os blocos para que o mesmo seja válido. O direito de ler o bloco pode ser público ou restrito aos participantes.

Segundo [Tapscott, 2016], Blockchains privados e permissionados parecem ter algumas vantagens claras em relação aos Blockchain públicos e não permissionados. Por um lado, seus membros podem facilmente mudar as regras do Blockchain, se assim o desejar. Os custos podem ser mantidos baixos, pois as transações precisam apenas da validação dos próprios membros, eliminando a necessidade de mineradores anônimos que consomem muita eletricidade nos processos de obtenção de consenso. Por fim, considerando que todas as partes envolvidas são confiáveis, um ataque de 51% (a ser abordado na seção 2.5.5) torna-se bastante improvável.

Na tabela 2.7 abaixo, apresentamos as quatro versões de Blockchain que surgem quando combinamos as restrições de leitura e escrita nas estruturas de dados do Blockchain.

Tabela 2.7 - Versões de Blockchain.

Acesso de escrita	**Acesso de leitura e criação de transações**	
	Todos	Restrito
Todos	Pública	Consórcio
Restrito	Semiprivada	Privada

Fonte: (Drescher, 2018, adaptado).

Ainda segundo [Tapscott, 2016], como toda tecnologia disruptiva, existem visões concorrentes no ecossistema Blockchain. Mesmo o centro do contingente Blockchain parece ter se dispersado em diferentes criptocampos, cada um defendendo uma agenda diferente. Existem atualmente cerca de 1.494 (um mil quatrocentos e noventa e quatro) criptoativos no mundo, onde o Bitcoin detém cerca de 33,5% (trinta e três e meio por cento) desse mercado, avaliado em mais de 589 (quinhentos e oitenta e nove) bilhões de dólares [Campos, 2018].

Na tabela 2.8 abaixo, apresentamos algumas variantes de Blockchain (*Side Chains*), que se diferem do modelo original do Bitcoin, com características diferentes, a depender do método de consenso adotado.

Tabela 2.8 - Variantes de Blockchain.

Blockchain	Descrição
BigChainDB	Um sistema de código aberto, que oferece possibilidade de blocos privados ou públicos, controle descentralizado, imutabilidade e transferência de ativos digitais. (www.bigchaindb.com)
Chain Core	Uma plataforma centralizada, voltada para o modelo bancário atual. Para a emissão e transferência de ativos financeiros em uma infraestrutura de blocos de permissão. (https://chain.com/technology/)
Corda	Uma plataforma distribuída do livro com consenso pluggable. Possibilidade de diversos tipos de consenso no mesmo ambiente. (https://www.corda.net/)
Credits	Uma estrutura de desenvolvimento para construir Ledgers distribuídos autorizados. (https://credits.vision/)
Domus Tower	Projetado para ambientes regulados, com capacidade de transmissão de mais de 1 milhão de transações por segundo. (http://domustower.com/)
Elements	Uma tecnologia de código aberto, de nível de protocolo, para estender a funcionalidade do Bitcoin. Proposta de blocos laterais (sidechain) ao Bitcoin. (https://elementsproject.org)
Ethereum	Uma plataforma descentralizada de cadeia de blocos, que executa contratos inteligentes e buscam outras funcionalidades. (www.ethereum.org)
Hyperledger Fabric	Uma plataforma para o desenvolvimento de aplicativos ou soluções com uma arquitetura modular, permite que componentes, como consenso e serviços de associação, sejam plug-and-play. (https://www.hyperledger.org/projects/fabric)

Blockchain	Descrição
Hyperledger Burrow (antigo Eris:db)	Um código aberto, tecnologia de nível de protocolo para estender a funcionalidade do Bitcoin. (www.hyperledger.org)
Hyperledger Iroha	Um sistema de contabilidade distribuída mais "simples" e modularizado, com ênfase no desenvolvimento de aplicações móveis. (https://www.hyperledger.org)
Hyperledger Sawtooth Lake	Um conjunto de blocos modulares em que a lógica de negócios de transações é desacoplada da camada de consenso. (https://www.hyperledger.org)
Multichain	Uma plataforma de código aberto, baseada no blockchain do Bitcoin, para transações financeiras multi-ativos. (www.multichain.com)
Namecoin	Uma tecnologia experimental de código aberto, que melhora a descentralização, a segurança, a censura, a privacidade e a velocidade de certos componentes da infraestrutura da Internet, como DNS e identidades. (https://namecoin.org/)
Openchain	Um sistema de contabilidade distribuída de código aberto, para emissão e gerenciamento de ativos digitais. (www.openchain.org)
Quorum	Um Ledger distribuído de código aberto e uma plataforma de contrato inteligente, baseada no Ethereum. e desenvolvida pelo banco JP Morgan. (https://www.jpmorgan.com/country/US/EN/Quorum)
Ripple	Sistema de liquidação bruta em tempo real (RTGS), câmbio e rede de remessas desenvolvido pela Ripple, baseado em um banco de dados público compartilhado,que usa um processo de consenso que permite pagamentos, trocas e remessas em um processo distribuído. (https://ripple.com/)
Stellar	Uma infraestrutura de pagamentos distribuídos de fonte aberta, que fornece servidores RESTful HTTP API que se conectam ao Stellar Core, a espinha dorsal da rede Stellar. (www.stellar.org)
Symbiont Assembly	Um livro distribuído inspirado por Apache Kafka. Possibilita troca de ativos. (https://symbiont.io)

Fonte: (Lyra e Meiriño, adaptado).

Como se pode verificar, existem redes mais ou menos indicadas para cada tipo de aplicação, o que nos leva a concluir que elas não concorrem entre si ou prejudicam o ecossistema como um todo, sendo mais complementares do que concorrentes. Segundo [Braga, 2017] a grande variedade de implementações disponíveis e de estudos empíricos

realizados, ou em andamento, dificultam saber qual a plataforma de Blockchain vai prevalecer.

2.5. QUESTÕES DE SEGURANÇA

Segundo [Drescher, 2018], a tecnologia Blockchain objetiva prover integridade e confiança em um sistema P2P totalmente aberto, composto de um número desconhecido de nós, com níveis de confiança e de confiabilidade desconhecidos. Desde a sua criação, a tecnologia Blockchain tem sido alvo de debates intensos sobre os seus aspectos de segurança, proporcionando diferentes pontos de vista de especialistas para continuar construindo e agregando valor a essa nova tecnologia. Apesar de contar com uma forte base teórica contra fraudes, ainda persistem dúvidas nas suas proteções para a realidade econômica digital. Neste contexto, e de acordo com [Braga, 2017], analisaremos 5 (cinco) aspectos de segurança envolvidos no estado da arte da tecnologia Blockchain, a saber: Segurança em camadas, Vulnerabilidades mais comuns, Confidencialidade e Anonimato, Segurança de Contratos Inteligentes e Ataques específicos contra Criptomoedas.

2.5.1. Segurança em camadas

O Blockchain, bem como as aplicações construídas com ele, devem adotar mecanismos de segurança baseados em camadas. Neste contexto, há 6 (seis) camadas de segurança a serem consideradas em uma aplicação Blockchain, a saber:

a) **Transação:** o Blockchain deve validar as transações com confiança e previsibilidade ao final do consenso. É o consenso que vai confirmar a finalidade e a imutabilidade da transação;

b) **Conta do usuário:** muitas vezes, a proteção da conta do usuário é confundida com a segurança do software cliente (*eWallets*). A conscientização dos usuários no uso seguro da tecnologia, e a implementação correta dos mecanismos de segurança para dispositivos móveis e sistemas web, são fatores decisivos para segurança nesta camada;

c) **Segurança da Aplicação e dos *Chaincodes*:** refere-se às boas práticas de desenvolvimento seguro de software, incluindo a codificação segura de contratos inteligentes, abordado na seção 2.3 (Contratos Inteligentes), e a definição de requisitos de segurança, avaliação da arquitetura e testes de segurança da aplicação;

d) **Segurança de implantação e de operação da aplicação:** são os testes de aceitação e homologação da aplicação e dos *chaincodes* antes da implantação e produção da aplicação.

Uma vez no ambiente de produção, a aplicação deve ser monitorada visando a detecção de anomalias de funcionamento e comportamento;

e) **Rede P2P:** são os mecanismos de proteção tradicionais das redes de computadores (firewall, IDS, IPS, etc.). Além disso, proteções específicas devem ser aplicadas para a segurança do protocolo de comunicação e de consenso. Por fim, também deve ser observada a quantidade mínima necessária de nós disponíveis para garantir o seu consenso;

f) **Governança da aplicação:** são as decisões sobre a estrutura e o projeto do Blockchain a ser implantado, que afetam o funcionamento com segurança, incluindo ainda controles antifraude, auditoria, privacidade e até conformidade às normas padrões específicas do nicho da aplicação.

2.5.2. Vulnerabilidades mais comuns

As vulnerabilidades ou bugs mais comuns em sistemas baseados na tecnologia Blockchain, em ordem decrescente de ocorrência, são: semânticos (na lógica da aplicação), ambiente e configurações, interface gráfica, concorrência, build, segurança, alocação de memória, desempenho, compatibilidade, e bifurcação da Ledger. Outros defeitos de segurança estão relacionados às ocorrências específicas de vulnerabilidades conhecidas, tais como: overflow de inteiros no timestamp de um bloco causado por um minerador malicioso, ataques por canal lateral de tempo (*timing attack*), viabilizado pelo modo como as senhas são comparadas na autenticação, diversas vulnerabilidades de SSL/TLS relacionadas à validação incompleta de certificados que facilitam ataques como o *padding oracle* e *BEAST*.

2.5.3. Confidencialidade e Anonimato

No Blockchain tradicional, a privacidade e a confidencialidade são limitadas por 2 (dois) aspectos, a saber:

a) **Pseudoanonimato da transação:** a rede Bitcoin não garante anonimato aos seus usuários, ao contrário do que se possa imaginar, mas sim a privacidade, o que é diferente. Dentro da rede, os usuários não são identificados por nome e número de identidade, mas por número de carteiras e chaves públicas. O anonimato, que antes era possível pela simples desconexão entre o endereço utilizado e seu real proprietário, já é ameaçado por técnicas de análise do Blockchain, com o objetivo específico de se descobrir os reais usuários por trás dos mesmos. Análise das correlações entre transações, os endereços de destino e outros metadados derivados da lógica da aplicação, podem facilitar a revelação da identidade do usuário;

b) **Transações em claro:** todas as transações contidas em um bloco estão em claro, isto é, sem criptografia para sigilo. A exploração de vulnerabilidades em carteiras eletrônicas, pode tanto facilitar o roubo de criptomoedas, como também revelar a identidade do usuário. Em *eWallets* de Bitcoin que utilizam o algoritmo criptográfico ECDSA para assinar transações, cada assinatura requer um número aleatório único e imprevisível. Porém, defeitos de segurança em algumas destas *eWallets*, na geração e utilização de números pseudoaleatórios ruins, podem resultar na revelação da chave privada a partir da geração de assinaturas digitais ECDSA repetidas, facilitando com isso, o roubo de Bitcoins e o rastreamento de transações assinadas com estas chaves inseguras.

2.5.4. Segurança de Contratos Inteligentes

Blockchain e contratos inteligentes (*chaincodes*) são tecnologias complexas que possuem vários benefícios quando usados isoladamente. A combinação destas tecnologias complexas, em vários contextos da aplicação, levanta novas preocupações com segurança relacionadas não apenas às tecnologias isoladas em seus casos de uso comuns, mas também emergentes das interações desconhecidas e até inesperadas entre estas tecnologias para resolver casos de uso incomuns (inovadores) em novas situações. A segurança de Contratos Inteligentes (*smart contracts*) é analisada por dois aspectos, a saber:

2.5.4.1. Defeitos de segurança

Comuns a várias plataformas de *smart contracts,* abordado na seção 2.3 (Contratos Inteligentes). Pesquisas apontam a existência de 4 (quatro) vulnerabilidades, a saber;

a) **Dependência da ordem de transações:** a ordem em que as transações são executadas por um contrato inteligente, pode alterar o resultado final deste *chaincode*. A vulnerabilidade TOD (*Transaction Ordering Dependence*) ocorre quando um nó malicioso altera a ordem em que as transações são executadas por um contrato, por exemplo, priorização de recebimentos em um ambiente de oscilação de valores, num sistema de pagamento;

b) **Dependência do carimbo de tempo:** há contratos que usam o carimbo de tempo da transação (*timestamp*) como gatilho ou condição para alguma operação crítica, por exemplo, na geração da chave privada do usuário;

c) **Tratamento defeituoso de exceções:** quando um contrato inteligente dispara outro, ele deve estar preparado para o caso excepcional do contrato chamado não terminar sua execução corretamente. Se esse término anormal não for tratado com a atenção devida, falhas no

contrato chamador podem ocorrer e até ser exploradas em ataques e fraudes. Por exemplo, um contrato de crédito, que faz a transferência de valores entre uma origem e um destino, não trata um determinado erro no contrato de débito, e credita o valor na conta de destino, apesar do erro no débito, sem debitar da conta de origem;

d) **Vulnerabilidade de código reentrante:** dois contratos mutuamente dependentes acessam estados intermediários, possivelmente inconsistentes um do outro. Se o primeiro contrato toma decisões de negócios com base em estados intermediários inconsistentes, a decisão tomada será incorreta. Esta situação pode ser explorada em fraudes e outros ataques.

2.5.4.2. Vulnerabilidades da Etherium

Trata-se da plataforma Blockchain de contratos inteligentes mais utilizada atualmente. Existem, basicamente, 3 (três) categorias de vulnerabilidades relacionadas a esta plataforma:

a) **Vulnerabilidades da Linguagem de programação Solidity:** são todas exploráveis em ataques que roubam *Ether* (a criptomoeda do *Ethereum*) de contratos. Em relação ao tratamento de exceções malfeito, alguns contratos não validam o retorno de funções. Campos privados de contratos podem ter seus valores públicos na Ledger, além disso, há casos de vulnerabilidade em código reentrante;

b) **Vulnerabilidades da máquina virtual Ethereum (Ethereum Virtual Machine - EVM):** há vulnerabilidades descobertas nos binários dos contratos inteligentes (*bytecodes*) que são implantados nos nós da rede P2P e executados pela *EVM*. Contratos já implantados são imutáveis, pois são vinculados a transações no Blockchain, então bugs são difíceis de corrigir e a sua recuperação pode ser drástica, por exemplo, com uma bifurcação (*hard fork*) na Ledger.

c) **Vulnerabilidades associadas ao Blockchain Ethereum:** como o Blockchain Ethereum gerencia contratos inteligentes, há também casos de vulnerabilidades relacionadas à dependência da ordem de transações e dependência do carimbo de tempo.

2.5.5. Ataques específicos contra Criptomoedas

Em que pese haver uma imutabilidade característica da estrutura de funcionamento da tecnologia Blockchain, abordada na seção 2.2 (Funcionamento do Blockchain), não podemos descartar a possibilidade de ataques específicos contra criptomoedas, particularmente o Bitcoin, por ser o mais popular. Assim, o conhecimento e a análise dos mesmos, são instrutivos para se evitar casos semelhantes em construções análogas. A maioria dos ataques,

que se tem conhecimento, se refere ao gasto repetido ou duplicado de Bitcoins (*double spending*). A seguir, apresentamos 4 (quatro) tipos de ataques já documentados e estudados:

a) **Ataque 51%:** conforme abordado na seção 2.2.3 (Validação / Mineração), e de acordo com a regra da maior cadeia (*Longest Chain Rule*), quando ocorrem duas transações duplicadas que usam o mesmo valor de origem, a primeira transação a entrar no Blockchain é considerada válida e a outra é descartada. Neste contexto, um atacante poderoso poderia substituir uma transação, que já entrou no Blockchain, por outra que usa o mesmo valor de origem. Um ataque de 51% ocorre no momento em que uma pessoa ou grupo de mineradores controla 51%, ou mais, do poder computacional da rede, uma vez que ele teria a mesma capacidade de mineração que todos os outros grupos de mineração, além de uma adição com a qual poderia atingir um ataque negativo a este sistema eletrônico distribuído, alterando temporariamente o funcionamento da rede. Neste caso, para substituir uma transação em um bloco, o atacante deveria minerar de novo o bloco corrente e os seus sucessores. Para tal, a sua capacidade de computação de valores hash (*hash rate*) tem que ser maior que a da rede P2P. Por isto, este ataque só é viável para um atacante que tem domínio da rede P2P, isto é, ele controla mais de 50% dos nós (ou da capacidade de hash) da rede. Este atacante poderoso poderia então sequestrar a rede, se recusando a minerar blocos de outros mineradores. Por isto, este também é um ataque contra outros mineradores;
b) **Ataque de competição (race attack):** neste tipo de ataque, transações duplicadas em nós diferentes da rede P2P, causam a falsa impressão de *double-spending,* devido a latência da rede e às diferenças de tempo de propagação de blocos, a partir de nós próximos ou de nós distantes. O *double spending* aparente só existe até que a transação entre em um bloco e este bloco alcance os nós da rede P2P. Os nós mais próximos percebem a duplicação antes dos nós mais distantes;
c) **Ataque do minerador malicioso (Finney Attack):** nesta modalidade, o atacante minera um bloco em segredo, com uma transação sua para si mesmo (autotransação), a qual não é difundida na rede P2P. Antes de liberar o bloco secreto, o atacante divulga outra transação duplicada, tendo como destino uma vítima, que aceita o pagamento sem confirmar o bloco (uma prática ruim), quando então, o atacante libera o bloco secreto antes que outro minerador ache o bloco com a transação de pagamento para a vítima, passando o seu pagamento na frente. Daí o termo *double-spending*;
d) **Spam ou enxurrada de transações (Transaction Spamming / flooding):** trata-se de um ataque de negação de serviço (*Denial of Service - DoS*) contra a rede P2P de um Blockchain.

Nesta modalidade, uma enxurrada de autotransações impede que os nós atacados processem outras transações. Análises indicam que este ataque não é viável no Bitcoin, principalmente, por 3 (três) motivos:

- Apenas poucas transações grátis são permitidas em um bloco;
- A taxa de serviço do minerador encarece o ataque;
- As transações de valor muito baixo são descartadas.

Todavia, esse tipo de ataque pode ser viável em outros tipos Blockchain com mecanismos de incentivo diferentes para o seu consenso.

Segundo [Drescher, 2018], a arma mais importante da tecnologia Blockchain contra nós desonestos é o poder da maioria honesta e os efeitos das recompensas e das punições. Mesmo que alguns nós enviem transações forjadas ou aceitem dados de transação ou blocos inválidos, a maioria dos nós honestos e seus esforços para receber recompensas superarão as tentativas dos nós desonestos que agirem contra a integridade do sistema.

2.6. PADRÕES GENÉRICOS DE APLICAÇÕES

Segundo [Drescher, 2018], sendo a tecnologia Blockchain um repositório de dados genérico, para todo o tipo de dados, com propriedades independentes do que armazena, sua aplicabilidade é bastante extensa, podendo ser utilizado em diversas áreas de aplicação. Com base em suas propriedades, identificamos os seguintes padrões de uso genérico desta tecnologia:

2.6.1. Prova de existência

São aplicações onde se tem como foco a armazenagem de dados com o propósito de comprovar a sua existência. Portanto, nem os recursos de ordenação, como o hash do bloco, nem os de timestamps do Blockchain são usados. Exemplos: registros de itens que se supõe serem únicos, como nomes de marcas, patentes, códigos de licença e endereços de internet ou de e-mail;

2.6.2. Prova de não existência

É o oposto da Prova de existência, onde as aplicações oferecem meios de se comprovar a inexistência de uma determinada informação. Exemplos: registro de reclamações, multas ou condenações;

2.6.3. Prova de tempo

São aplicações onde não só a existência de uma determinada informação é importante, mas também o instante em que ela foi criada. Exemplos: monitoração de entregas ou de notificações, de pagamentos, de abertura e encerramento ordenados de procedimentos de licitações públicas e gerenciamento de previsões;

2.6.4. Prova de ordem

São aplicações que monitoram a ordem relativa da ocorrência de determinados eventos, independentemente dos seus horários absolutos. Exemplos: monitoração de processos de matrículas, auditoria de procedimentos de licitações públicas, matrículas em escolas, solicitações de patentes ou reinvindicações de direitos autorais;

2.6.5. Prova de identidade

São aplicações específicas à Prova de existência, porque comprova que uma determinada identidade já existe, além de provê conceitos básicos de segurança para identificação e autenticação. Exemplos: documentos de identidade digitais para pessoas, animais ou bens, carteiras de habilitação ou passaportes;

2.6.6. Prova de autoria

São aplicações que tem como foco provar que uma pessoa ou instituição específica adicionou determinados dados no Blockchain. Conforme já abordado, a tecnologia Blockchain só permite operações de escrita, em sua estrutura de dados, após a identificação, autenticação e autorização do usuário. Exemplo: publicações eletrônicas, monitoração de mudanças de conteúdo em documentos, entrega de conteúdo, edição colaborativa e proteção de direitos autorais;

2.6.7. Prova de posse

São aplicações que tem como foco a prova da posse de um determinado ativo. Elas dependem de todos os padrões mencionados anteriormente. Exemplos: sistemas de gerenciamento de posses de imóveis, carros, ações de empresas, títulos e dinheiro digital ou criptomoedas.

2.7. CASOS DE USO

Existem, atualmente, diversas áreas de negócio que poderão ser impactadas e modificadas com ganhos de eficiência pela tecnologia do Blockchain. Na realidade, qualquer ramo de atividade, público ou privado, comercial ou industrial, que necessite de registro ou certificação, pode se beneficiar dessa tecnologia. No entanto, é consenso entre os analistas e desenvolvedores que trabalham com a tecnologia, que ela ainda está em seu início, precisando superar alguns desafios para que seja popularizada, necessitando se adaptar às particularidades de cada setor e às necessidades de cada negócio e seus stakeholders. Ela não é estática, a qual uma vez desenvolvida, permanecerá inalterada pelo resto de sua existência, pelo contrário, é a base do que já foi, e continuará sendo tema de pesquisas, melhorias e novos desenvolvimentos. Podemos abordar esse processo por 3 (três) visões distintas:

- Pequenas melhorias e variações técnicas;
- Melhoria na escalabilidade;
- Evoluções conceituais e alternativas.

Assim, a cada nova aplicação, é fundamental que se passe por etapas de PoC (prova de conceito) e MVP (mínimo produto viável). Essas etapas servem para minimizar os seus custos, diminuindo assim, a sua escala para testes e validações. A seguir, apresentamos 4 (quatro) exemplos de áreas de aplicação concretas da tecnologia Blockchain, nas quais ela já está sendo, ou prestes a ser usada:

2.7.1. Rastreamento de ativos

São aplicações que se utilizam da funcionalidade de rastreamento de ativos que a tecnologia Blockchain permite. Isso significa que podemos rastrear um produto ou uma certificação desde a sua origem, seja o produto que for: de luxo, de beleza, um pedaço de terra etc. Como caso prático, podemos citar o do Walmart, onde em outubro de 2016, foi testado um sistema de rastreamento de produtos alimentícios, para identificar erros nos processos e a origem de produtos de má qualidade. A PoC utilizou dois produtos, um de origem nos Estados Unidos, outro da China para mostrar, com sucesso, como seria possível seu rastreamento. Exemplo: monitoramento da comida que você consome em casa até o fazendeiro ou produtor que cultivou esse alimento.

2.7.2. Identidade Digital

São aplicações que comprovam a identidade e fazem a autenticação com base em itens digitais únicos. Anônimos, pseudônimos ou identidades reais podem ser mapeados na tecnologia Blockchain. Isso significa que, se você tiver a sua identidade registrada no Blockchain, ela poderá funcionar como um cadastro único ao qual apenas as empresas ou organizações autorizadas terão acesso. Um dos maiores benefícios do Blockchain é tornar possível o registro e a certificação desse tipo de informação, garantindo a legitimidade das informações fornecidas. Assim, uma vez que o documento é gravado na rede, esta funcionalidade trará grandes benefícios para negócios cuja conferência de dados é parte fundamental da atividade, com o intuito de eliminar fraudes. Como caso prático, podemos citar o do Civic.

2.7.3. Internet das coisas

Conforme definido na Wikipédia, a Internet das Coisas (do inglês, *Internet of Things, IoT*) é uma rede de objetos físicos, veículos, prédios e outros que possuem tecnologia embarcada, sensores e conexão com a rede e é capaz de coletar e transmitir dados. Um grande problema associado à *IoT,* são os aspectos relacionados à segurança e privacidade. A utilização da tecnologia Blockchain pode contribuir para a mitigação desse problema. Segundo [Tapscott, 2016], nesse mundo tudo é identificado, e o Blockchain é a base para a *IoT,* é a estrutura que facilita o processamento de transações e coordenação entre os dispositivos que interagem. A *IoT* não pode funcionar sem redes de pagamento Blockchain, onde o Bitcoin é a linguagem transacional universal. Nesse mundo emergente, os usuários se conectam com dispositivos inteligentes, usando identificação e autenticação seguras, chaves potencialmente públicas/privadas, e elas definem as regras de engajamento, como a privacidade com outros dispositivos, em vez de aceitarem as regras de um nó centralizado. A título de ilustração, seguem alguns exemplos potenciais de utilização da tecnologia:

a) Rastrear a história única de cada dispositivo, registrando a troca de dados com outros dispositivos, serviços web e usuários humanos;

b) Permitir que dispositivos inteligentes atuem de forma autônoma em uma variedade de transações. Como exemplos, podemos citar:

- Monitoramento remoto de ativos de elevado valor para se verificar, por exemplo, se estão sendo usados corretamente;

- Monitoramento, controle e autorização de solicitação de determinado equipamento para reposição de alguma peça ou matéria-prima (máquina de lavar solicitando sabão, por exemplo);
- Controle de identidade dos dispositivos *IoT* para registro e controle de acesso lógico a diferentes aplicações.
- Uma casa com integração dos aparelhos eletrônicos ligados a uma rede, Wifi ou Bluetooth, por exemplo. Com um sistema integrado, é possível ter o controle de muitas coisas, como a iluminação, temperatura, ativação de eletrodomésticos, como programar a torradeira para o horário que você costuma acordar ou preparar um cafezinho para quando você estiver chegando em casa.

2.7.4. Governos

Em vários países, a tecnologia Blockchain já está revolucionando a máquina administrativa, tornando-a mais eficiente e criando novas oportunidades de mudança da democracia. Benefícios da tecnologia, tais como maior transparência, redução de fraudes, e compartilhamento de dados, favorecem o desenvolvimento de várias aplicações de extrema importância para o governo. Seguem alguns exemplos:

a) **Votação eletrônica:** pode ser utilizada para impossibilitar a realização de dois votos pela mesma pessoa e a garantir a imutabilidade dos registros das zonas eleitorais;
b) **Gestão de identidade de pessoas:** permite a implantação de programas confiáveis, de abrangência nacional, para a gestão de identidade digital dos cidadãos, permitindo o registro seguro através de parâmetros biométricos;
c) **Controle de acesso:** controle de acesso lógico e físico de diferentes serviços públicos, e órgãos da administração, com caraterísticas de rastreabilidade e imutabilidade de registros;
d) **Pagamento de programas sociais:** permite a implantação de programas sociais com o rastreamento de recursos distribuídos;
e) **Controle de ativos:** implantação de sistemas de controle de ativos, em diferentes níveis da administração, mantendo o histórico de vida dos ativos cadastrados, desde o momento da sua compra até o seu descarte.

Vários governos ao redor do mundo trabalham com diferentes iniciativas de aplicações. Seguem algumas das mais conhecidas:

- **Estônia:** BitNation serviço notarial público, e-residency program com digital ID, e-Escola para acompanhar tarefas, currículo e notas, i-Voting para votações e plano de saúde com registros médicos rastreados;
- **Ucrânia:** plataforma de eleição que permite diversos níveis de eleição, petições online e referendos;
- **Suécia:** registro de transações imobiliárias;
- **Reino Unido:** distribuição de benefícios, departamento de trabalho e pensões;
- **Brasil:** compartilhamento da base de dados do CPF, mais simples e transparente, através do serviço b-CPF.

O capítulo 3 (Aplicação do Blockchain na área de Trânsito), apresenta uma proposta de utilização da tecnologia no processo de registro de arrecadação de infrações de trânsito em nosso país.

2.8. OBSTÁCULOS E DESAFIOS DE IMPLEMENTAÇÃO

Por todo o exposto, a tecnologia Blockchain é um sistema ponto a ponto puramente distribuído, permitindo, a princípio, que todos leiam e adicionem novos dados à sua Ledge. Isto lhe confere uma construção técnica complexa e extremamente sofisticada, calcada fundamentalmente na sua natureza aberta e na ausência de intermediários no seu controle. Entre as inúmeras vantagens de utilização do Blockchain, podemos destacar a redução de custos, assegurando um maior nível de confiança das informações, eliminando despesas de intermediários e validando todas as informações com uma segurança nunca vista antes. No entanto, ela não é perfeita e nem está livre de limitações, ainda existem diversos desafios a serem superados, segundo [Mougayar, 2017] algumas barreiras precisam ser transpostas, como a capacidade de processamento de grandes volumes de informação, o tempo necessário para que as transações sejam registradas na rede, permissionamento e anonimato, integração de diferentes partes envolvidas em um mesmo novo modelo operacional, entre outros. Segundo a [Cedro Technologies], a tecnologia Blockchain é algo ainda recente e altamente inovadora, e diante de sua complexidade e potencial, certamente ela ainda enfrentará alguns desafios relacionados à sua regulação e à quebra de paradigmas para sua adoção prática, bem como, dificuldades técnicas e deficiências, que a tecnologia apresenta, que precisarão ser superadas para que se possa ganhar a plena confiança das pessoas e espaço na economia global. Didaticamente falando, existem 3 (três) grupos de desafios, a saber:

2.8.1. Desafios técnicos e falhas na segurança

Um dos maiores desafios que o Blockchain apresenta, está relacionado à segurança de suas transações, abordado na seção 2.5 (Questões de Segurança), bem como o seu desempenho quanto à velocidade de processamento das suas transações. Apresentamos a seguir, alguns exemplos:

a) Como sabemos, a princípio todos os dados do Blockchain estão acessíveis a qualquer usuário numa rede pública. Esta característica é fundamental para que se possa conferir a veracidade e a autenticidade das suas informações. Assim, a falta de privacidade pode ser considerada um fator limitante para casos de aplicações que demandem essa caraterística;

b) A tecnologia Blockchain utiliza criptografia assimétrica para identificação, autenticação de usuários e autorização de transações. Em que pese tratar-se de um dos melhores e mais robustos métodos de criptografia, conferindo à mesma um alto nível de segurança dos seus dados, não há mecanismos de proteção contra perda ou o compartilhamento indesejado da chave privada com terceiros, conferindo assim um fator limitante quanto ao seu uso;

c) Como a cadeia de blocos criptografados ganha mais força conforme a adição de novos blocos, as transações mais recentes não possuem uma segurança tão fortificada quanto as mais antigas. Tanto é que a recomendação específica para o uso do Bitcoin é a de se aguardar algumas horas para que novos blocos sejam adicionados à cadeia, para garantir que a sua transação não vá sofrer ataques, e com isso, invalidada;

d) Outro desafio a ser superado é a capacidade computacional necessária para gerar força o suficiente para que a Ledger da aplicação seja constantemente alimentada com dados validados por consenso. Por isso, o Bitcoin, possui uma janela de criação de blocos de transações de cerca de 10 minutos, quando todas as transações realizadas são verificadas, liberadas e armazenadas em um bloco que está ligado ao bloco anterior, criando assim uma corrente

e) O Blockchain é uma tecnologia que foi criada e construída para ser segura e não rápida. A taxa de criação de seus blocos (1/10 min) e seu tamanho máximo (1 MB ~ 1.000.000 bytes) são mantidos em níveis relativamente baixos, pelo protocolo Bitcoin, para garantir suficiente tempo de sua propagação a toda rede antes da produção de um novo bloco. Essas limitações restringem severamente a capacidade de transações (~ 250 bytes) na rede como um todo. A atual rede Bitcoin suporta no máximo uma média de 7 (sete) transações por segundo, valor muito abaixo que qualquer sistema tradicional de pagamentos online. Como comparação, a empresa Visa Inc. é capaz de lidar com um máximo de 56.000 transações por segundo. Se

pensarmos na expansão do uso da criptomoeda ou em sistemas robustos em redes menores, como as corporativas, o processo pode ser tão lento que se torne ineficiente. Essa característica, portanto, é considerada um obstáculo sério para aplicações que exijam velocidade de processamento, escalabilidade e throughput altos;

f) Uma das principais características do Blockchain é a sua imutabilidade, ou seja, ele não pode ser revertido, o que teoricamente significa que qualquer erro, seja o menor deles, não poderá ser corrigido;

g) O aumento de valor da moeda bitcoin no mercado atrai cada vez mais o interesse dos mineradores, e consequentemente, mais processamento e mais consumo de energia. Atualmente, a energia que é consumida pelo sistema do Blockchain é insustentável. A título de ilustração, em 2017, a rede Bitcoin consumiu aproximadamente 35 TWh, o equivalente ao consumo de um pequeno país como a Bulgária. Hoje temos grande parte da mineração do Bitcoin na China, pois lá a energia é barata e subvencionada pelo governo. Ao analisarmos o consumo de energia em um país como o Brasil, o desenvolvimento do Blockchain teria um custo muito alto;

h) De acordo com dados da União Internacional de Telecomunicações, ainda existem lacunas significativas na conectividade com a Internet, seja por causa da infraestrutura pobre de comunicação ou porque o serviço é inviável;

i) O Blockchain é uma construção técnica complexa constituída de vários componentes. Alterar este mecanismo pode ser muito desafiador, tornando todo o conjunto de tecnologias envolvidas, menos flexível em comparação com outras;

j) O Blockchain é com certeza um matador de empregos, uma vez que ele é uma plataforma extraordinária para automação radical, em que códigos de computador fazem o trabalho de seres humanos, gerenciando ativos e pessoas.

2.8.2. Desafios regulatórios e jurídicos

Esses desafios dizem respeito à falta de confiança que a tecnologia Blockchain apresenta junto aos mecanismos tradicionais de regulação e de tutela, como governos e bancos, a saber:

a) Devido ao seu poder de privacidade, a tecnologia Blockchain tem sido muito questionada por conta de seu uso por sonegadores de impostos, grupos terroristas, hackers e criminosos para lavagem de dinheiro e para esconder suas transações, mantendo o anonimato entre as partes envolvidas numa transação. Ao mesmo tempo em que a privacidade é uma característica

positiva da tecnologia, é também um obstáculo em processos investigativos, onde não há uma entidade a quem se possa recorrer para a quebra de sigilo. Contudo, é inegável a importância de adoção de políticas de compliance para prevenção desses tipos de ilícitos;

b) As legislações e os governos da maioria dos países ainda não reconhecem as criptomoedas ou as certificações digitais sem a participação de uma autoridade validadora legalmente reconhecida;

c) No Brasil, tramita na Câmara dos Deputados, um Projeto de Lei (PL nº 2303/2015), de autoria do Deputado Áureo (PSD/RJ), que dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de "arranjos de pagamento" sob a supervisão do Banco Central;

d) A Receita Federal do Brasil (RFB), para efeitos de tributação, define que as criptomoedas são equiparadas a ativos financeiros, já a Comissão de Valores Mobiliários (CVM) entende que não, o que denota que os órgãos reguladores no Brasil estão encontrando dificuldades em definir a natureza desse instituto. Juridicamente, segundo [Campos, 2018], não se trata de moeda, já que no Brasil apenas é considerada moeda aquela de curso forçado, emitida pelo Banco Central, de acordo com o Decreto-Lei 857, de 11 de setembro de 1969, que atualmente é o Real. Alguns Bancos Centrais já manifestaram interesse em criar suas próprias moedas virtuais como a Venezuela, com a criação do "Petros", e a Rússia, com o "Criptorublo";

e) Segundo [Campos, 2018], alguns países já regulamentaram o uso de criptoativos, outros ainda não o fizeram, apesar de não proibirem seu uso, enquanto alguns poucos decretaram sua ilegalidade no território:

- Países que declararam o Bitcoin e outras criptomoedas ilegais: Bangladesh, Bolívia, Equador, Kirziquistão e Argélia;

- Países que criaram algum tipo de regulamentação: Austrália, Canadá, China, Estados Unidos, Japão e Rússia.

Segundo [Campos, 2018], seria muito mais produtivo e inovador o desenvolvimento de uma auto-regulamentação para o setor, do que simplesmente tentar encaixá-lo no sistema existente, dado a especificidade do assunto e mesmo sua natural incompatibilidade com o sistema financeiro tradicional, centralizado e monopolista. Resta aguardar o final desse processo legislativo. É certo, no entanto, que toda essa turbulência no processo de regulamentação gera insegurança e angústia nos empreendedores do setor, além de

demonstrar o quanto o Poder Legislativo do nosso país está atrasado e em dissonância com os demais países desenvolvidos.

2.8.3. Desafios de aceitação dos usuários

O uso da tecnologia requer um certo nível de instrução de seus usuários. A alfabetização é muito desigual no mundo em desenvolvimento, a saber:

a) Um status legal em aberto, e não definido para o Blockchain, causará incertezas entre os seus usuários, reduzindo assim, o seu interesse em usá-lo. Iniciativas educativas sobre o funcionamento de novas tecnologias aumentam a sua aceitação e a adoção entre os usuários, além de promover a solução das questões legais;

b) Como qualquer tecnologia, o Blockchain pode ser utilizado com propósitos beneficentes ou malévolos. É fundamental e necessário que haja iniciativas de instituições, como organizações da sociedade civil, empresas, academia e governo, que possam alavancar esta tecnologia para o bem, disseminando-a como um instrumento de prosperidade global e da mudança positiva com sua infinidade de benefícios em prol do cidadão.

Esses desafios, inevitavelmente, trazem consigo um futuro bastante imprevisível quanto ao reconhecimento público da segurança dos documentos e transações gerados com a tecnologia Blockchain. Segundo [Campos, 2018], o que vai garantir adesão e sucesso a esse novo ativo será a confiança que o mercado depositará no novo protocolo criado, já que o valor das criptomoedas está totalmente relacionado à lei da oferta e procura.

3 APLICAÇÃO DO BLOCKCHAIN NA ÁREA DE TRÂNSITO

É um consenso recorrente afirmar que quando se trata de eficiência, salvo algumas exceções, os serviços e as operações de governo têm ainda um longo caminho a percorrer para o atingimento de uma excelência. Eles, em geral, estão organizados em departamentos que não compartilham suas informações. A burocracia com demasiada frequência triunfa sob o bom senso ou práticas compartilhadas. Os cidadãos raramente tem um único local para acessar serviços governamentais. Todo país possui um número incontável de políticos e burocratas desperdiçando dinheiro do contribuinte. O potencial para melhorar todas as interfaces da administração pública, agregando integridade e transparência aos governos junto a sociedade é significativo [Tapscott, 2016].

Por tudo que foi abordado até aqui, é inconteste que a tecnologia Blockchain possui características extremamente interessantes a ser aplicada no setor público. Ela garante segurança e transparência, em tempos delicados, onde a informação é o grande valor da sociedade. Trata-se portanto de uma tecnologia que permite a implementação de registros distribuídos, auditáveis e não fraudáveis. A ideia de se ter uma base de dados distribuída, ou seja, presente em todos os computadores participantes da rede, com mais segurança do que numa base centralizada, torna-se atraente e estimulante para que os governos caminhem nessa direção. O motivo principal do porque esta tecnologia é tão adequada para o uso no setor governamental é exatamente o seu conceito de transparência, com conteúdo auditável e não fraudável. Uma outra vantagem é o fato de que qualquer alteração nessas estruturas, demanda consenso de todos os envolvidos, o que torna difícil a manipulação indevida de seus dados. Por fim, outro argumento a favor do uso da tecnologia Blockchain no setor público é a de que ela não é excludente, e consegue integrar-se de forma independente com outros sistemas de computação já implantados, não exigindo nenhuma mudança nos seus sistemas atuais.

A legislação de trânsito brasileira está expressa na Constituição Federal (CF), de 5 de outubro de 1988, especificamente nos artigos 22, 23 e 144; no Código de Trânsito Brasileiro (CTB), objeto da Lei nº 9.503, de 23 de setembro de 1997, e suas alterações; em Portarias do DENATRAN, e em Resoluções e Deliberações do Conselho Nacional de Trânsito (CONTRAN). O CTB, preconiza que o trânsito, em condições seguras, é um direito de todos e dever dos órgãos e entidades componentes do Sistema Nacional de Trânsito (SNT), a estes cabendo, no âmbito de suas respectivas competências, adotar medidas destinadas a assegurar esse direito. Segundo [Pellizzon, 2017], o trânsito no Brasil está organizado pelos órgãos e entidades componentes do SNT, conforme sintetiza a tabela 3.1 abaixo. O SNT é o conjunto de órgãos e entidades da União, dos Estados, do Distrito Federal e dos Municípios que tem

por finalidade o exercício das atividades de planejamento, administração, normatização, pesquisa, registro e licenciamento de veículos, formação, habilitação e reciclagem de condutores, educação, engenharia, operação do sistema viário, policiamento, fiscalização, julgamento de infrações e de recursos e aplicação de penalidades.

Nesse sentido, o CTB em seu artigo 19, incisos VIII, IX e XXX, estabelece algumas competências ao DENATRAN, a saber:

...;

Art. 19. Compete ao órgão máximo executivo de trânsito da União:

VIII - organizar e manter o Registro Nacional de Carteiras de Habilitação - RENACH;

IX - organizar e manter o Registro Nacional de Veículos Automotores - RENAVAM;

XXX - organizar e manter o Registro Nacional de Infrações de Trânsito (RENAINF).

...;

Tabela 3.1 - Composição do Sistema Nacional de Trânsito.

Instância	**Órgãos Consultivos e Coordenadores**	**Órgãos Executivos**		**Agentes de Fiscalização**	**Julgamento de Recursos**	
		Trânsito	**Rodoviário**		**1ª Instância**	**2ª Instância**
Federal	CONTRAN	DENATRAN (CTB Art. 19)	DNIT e ANTT (CTB Art. 21)	DNIT, ANTT e PRF	JARI	Órgão Especial da JARI e CONTRAN
Estadual	CETRAN e CONTRANDIFE	DETRAN (CTB Art. 22)	DER (CTB Art. 21)	PM – Agente de Trânsito, DETRAN e DER (mediante convênio)	JARI	CETRAN e CONTRANDIFE
Municipal		Órgão Municipal de Trânsito (CTB Art. 24)	Órgão Municipal Rodoviário de Trânsito (CTB Art. 21)	PM (mediante convênio e/ou Agentes de Trânsito Municipal ou Guardas Municipais)	JARI	CETRAN e CONTRANDIFE

Fonte: (Pellizzon, 2017).

Trata-se, portanto de 3 (três) bases de dados centralizadas e atualmente mantidas pelo DENATRAN, através do Serviço Federal de Processamento de Dados (SERPRO), cuja atualização é descentralizada e de competência dos órgãos que compõem o SNT (Art. 7º do CTB). Como se pode verificar na tabela 3.1 acima, os órgãos com competência de executar a fiscalização do trânsito nas vias e rodovias, aplicando notificações de autuação e de penalidades, e arrecadando multas, a saber: os Executivos de Trânsito e Rodoviários, bem como os seus Agentes de Fiscalização, estão distribuídos nas instâncias Federal, Estadual e Municipal do nosso país.

Por motivos de facilidade de acesso às informações, exiguidade de tempo, e de economicidade, optou-se para este trabalho, pela pesquisa e levantamento de dados restrito aos órgãos que compõem o SNT, com sede no Distrito Federal, entendendo que esta amostragem de informações, obtidas junto a estas entidades, reflete a realidade nacional.

Segundo informações obtidas junto ao DER/DF, DETRAN/DF, DENATRAN, DNIT, PRF e o próprio SERPRO, existem dificuldades de ordem técnica e política na consulta e atualização dessas bases de dados centralizadas a tempo e hora necessárias, acarretando com isso, desconforto e prejuízo para o seu usuário principal: o cidadão. Nas seções a seguir, apresentamos, à luz do CTB, como se integram os órgãos em âmbito nacional, e como é operacionalizado o arcabouço de leis e normas relativas ao processo de manutenção dessas bases.

3.1. REGISTRO NACIONAL DE CARTEIRAS DE HABILITAÇÃO (RENACH)

Trata-se de um sistema coordenado pelo DENATRAN, que registra todo o histórico de cada motorista habilitado no Brasil. Ele abrange todos os eventos relacionados ao cidadão como motorista e inclui informações sobre habilitação, exames, carteira nacional de habilitação, infrações, penalidades e outros. Tais informações são geralmente registradas pelos órgãos e entidades que compõem o SNT, em conformidade com o CTB em seus artigos 140, 147, 159 e 290, a saber:

Art. 140. A habilitação para conduzir veículo automotor e elétrico será apurada por meio de exames que deverão ser realizados junto ao órgão ou entidade executivos do Estado ou do Distrito Federal, do domicílio ou residência do candidato, ou na sede estadual ou distrital do próprio órgão, devendo o condutor preencher os seguintes requisitos:

...;

Parágrafo único. As informações do candidato à habilitação serão cadastradas no RENACH.

...;

Art. 147. O candidato à habilitação deverá submeter-se a exames realizados pelo órgão executivo de trânsito, na seguinte ordem:

I - de aptidão física e mental;

II - (VETADO)

III - escrito, sobre legislação de trânsito;

IV - de noções de primeiros socorros, conforme regulamentação do CONTRAN;

V - de direção veicular, realizado na via pública, em veículo da categoria para a qual estiver habilitando-se.

§ 1º Os resultados dos exames e a identificação dos respectivos examinadores serão registrados no RENACH. (Renumerado do parágrafo único pela Lei nº 9.602, de 1998)

...;

Art. 159. A Carteira Nacional de Habilitação, expedida em modelo único e de acordo com as especificações do CONTRAN, atendidos os pré-requisitos estabelecidos neste Código, conterá fotografia, identificação e CPF do condutor, terá fé pública e equivalerá a documento de identidade em todo o território nacional.

...;

§ 6º A identificação da Carteira Nacional de Habilitação expedida e a da autoridade expedidora serão registradas no RENACH.

§ 7º A cada condutor corresponderá um único registro no RENACH, agregando-se neste todas as informações.

...;

Art. 290. Implicam encerramento da instância administrativa de julgamento de infrações e penalidades: (Redação dada pela Lei nº 13.281, de 2016)

...;

Parágrafo único. Esgotados os recursos, as penalidades aplicadas nos termos deste Código serão cadastradas no RENACH.

3.2. REGISTRO NACIONAL DE VEÍCULOS AUTOMOTORES (RENAVAM)

Trata-se de um sistema coordenado pelo DENATRAN, que registra todo o histórico do veículo, desde sua fabricação até o dia de seu descarte. Ele armazena todas as informações do veículo como características, multas, emplacamento, licenciamento, mudanças de proprietários, furtos e etc. Tais infrações são geralmente registradas pelos órgãos e entidades

que compõem o SNT, em conformidade com o CTB em seus artigos 103, 119, 122, 123, 124, 125, 127, 257 e 270, a saber:

Art. 103. O veículo só poderá transitar pela via quando atendidos os requisitos e condições de segurança estabelecidos neste Código e em normas do CONTRAN.

§ 1º Os fabricantes, os importadores, os montadores e os encarroçadores de veículos deverão emitir certificado de segurança, indispensável ao cadastramento no RENAVAM, nas condições estabelecidas pelo CONTRAN.

...;

Art. 119. As repartições aduaneiras e os órgãos de controle de fronteira comunicarão diretamente ao RENAVAM a entrada e saída temporária ou definitiva de veículos.

...;

Art. 122. Para a expedição do Certificado de Registro de Veículo o órgão executivo de trânsito consultará o cadastro do RENAVAM e exigirá do proprietário os seguintes documentos:

...;

Art. 123. Será obrigatória a expedição de novo Certificado de Registro de Veículo quando:

...;

§ 3º A expedição do novo certificado será comunicada ao órgão executivo de trânsito que expediu o anterior e ao RENAVAM.

...;

Art. 124. Para a expedição do novo Certificado de Registro de Veículo serão exigidos os seguintes documentos:

...;

VII - certidão negativa de roubo ou furto de veículo, expedida no Município do registro anterior, que poderá ser substituída por informação do RENAVAM;

...;

Art. 125. As informações sobre o chassi, o monobloco, os agregados e as características originais do veículo deverão ser prestadas ao RENAVAM:

...;

Parágrafo único. As informações recebidas pelo RENAVAM serão repassadas ao órgão executivo de trânsito responsável pelo registro, devendo este comunicar ao RENAVAM, tão logo seja o veículo registrado.

...;

Art. 127. O órgão executivo de trânsito competente só efetuará a baixa do registro após prévia consulta ao cadastro do RENAVAM.

...;

Parágrafo único. Efetuada a baixa do registro, deverá ser esta comunicada, de imediato, ao RENAVAM.

...;

Art. 257. As penalidades serão impostas ao condutor, ao proprietário do veículo, ao embarcador e ao transportador, salvo os casos de descumprimento de obrigações e deveres impostos a pessoas físicas ou jurídicas expressamente mencionados neste Código.

...;

§ 10. O proprietário poderá indicar ao órgão executivo de trânsito o principal condutor do veículo, o qual, após aceitar a indicação, terá seu nome inscrito em campo próprio do cadastro do veículo no RENAVAM.(Incluído pela Lei nº 13.495, 2017)

§ 11. O principal condutor será excluído do RENAVAM: (Incluído pela Lei nº 13.495, 2017)

I - quando houver transferência de propriedade do veículo; (Incluído pela Lei nº 13.495, 2017)

II - mediante requerimento próprio ou do proprietário do veículo;(Incluído pela Lei nº 13.495, 2017)

III - a partir da indicação de outro principal condutor. (Incluído pela Lei nº 13.495, 2017)

...;

Art. 270. O veículo poderá ser retido nos casos expressos neste Código.

...;

§ 6º Não efetuada a regularização no prazo a que se refere o § 2º, será feito registro de restrição administrativa no RENAVAM por órgão ou entidade executivo de trânsito dos Estados e do Distrito Federal, que será retirada após comprovada a regularização. (Incluído pela Lei nº 13.160, de 2015).

3.3. REGISTRO NACIONAL DE INFRAÇÕES DE TRÂNSITO (RENAINF)

Trata-se de um sistema coordenado pelo DENATRAN, que registra todas as infrações cometidas pelos usuários do trânsito Brasileiro, em qualquer Unidade da Federação (UF), independentemente onde o veículo esteja registrado. Tais infrações são geralmente registradas pelos órgãos e entidades que compõem o SNT, em conformidade com o CTB em seus artigos 20, 21, 22 e 24, a saber:

Art. 20. Compete à Polícia Rodoviária Federal, no âmbito das rodovias e estradas federais:

...;

III - aplicar e arrecadar as multas impostas por infrações de trânsito, as medidas administrativas decorrentes e os valores provenientes de estada e remoção de veículos, objetos, animais e escolta de veículos de cargas superdimensionadas ou perigosas;

...;

X - integrar-se a outros órgãos e entidades do Sistema Nacional de Trânsito para fins de arrecadação e compensação de multas impostas na área de sua competência, com vistas à unificação do licenciamento, à simplificação e à celeridade das transferências de veículos e de prontuários de condutores de uma para outra unidade da Federação;

...;

Art. 21. Compete aos órgãos e entidades executivos rodoviários da União, dos Estados, do Distrito Federal e dos Municípios, no âmbito de sua circunscrição:

...;

VI - executar a fiscalização de trânsito, autuar, aplicar as penalidades de advertência, por escrito, e ainda as multas e medidas administrativas cabíveis, notificando os infratores e arrecadando as multas que aplicar;

...;

VIII - fiscalizar, autuar, aplicar as penalidades e medidas administrativas cabíveis, relativas a infrações por excesso de peso, dimensões e lotação dos veículos, bem como notificar e arrecadar as multas que aplicar;

IX - fiscalizar o cumprimento da norma contida no art. 95, aplicando as penalidades e arrecadando as multas nele previstas;

...;

XII - integrar-se a outros órgãos e entidades do Sistema Nacional de Trânsito para fins de arrecadação e compensação de multas impostas na área de sua competência, com vistas à unificação do licenciamento, à simplificação e à celeridade das transferências de veículos e de prontuários de condutores de uma para outra unidade da Federação;

...;

Art. 22. Compete aos órgãos ou entidades executivos de trânsito dos Estados e do Distrito Federal, no âmbito de sua circunscrição:

...;

VI - aplicar as penalidades por infrações previstas neste Código, com exceção daquelas relacionadas nos incisos VII e VIII do art. 24, notificando os infratores e arrecadando as multas que aplicar;

...;

XIII - integrar-se a outros órgãos e entidades do Sistema Nacional de Trânsito para fins de arrecadação e compensação de multas impostas na área de sua competência, com vistas à unificação do licenciamento, à simplificação e à celeridade das transferências de veículos e de prontuários de condutores de uma para outra unidade da Federação;

XIV - fornecer, aos órgãos e entidades executivos de trânsito e executivos rodoviários municipais, os dados cadastrais dos veículos registrados e dos condutores habilitados, para fins de imposição e notificação de penalidades e de arrecadação de multas nas áreas de suas competências;

...;

Art. 24. Compete aos órgãos e entidades executivos de trânsito dos Municípios, no âmbito de sua circunscrição: (Redação dada pela Lei nº 13.154, de 2015)

...;

VI - executar a fiscalização de trânsito em vias terrestres, edificações de uso público e edificações privadas de uso coletivo, autuar e aplicar as medidas administrativas cabíveis e as penalidades de advertência por escrito e multa, por infrações de circulação, estacionamento e parada previstas neste Código, no exercício regular do poder de polícia de trânsito, notificando os infratores e arrecadando as multas que aplicar, exercendo iguais atribuições no âmbito de edificações privadas de uso coletivo, somente para infrações de uso de vagas reservadas em estacionamentos; (Redação dada pela Lei nº 13.281, de 2016)

VII - aplicar as penalidades de advertência por escrito e multa, por infrações de circulação, estacionamento e parada previstas neste Código, notificando os infratores e arrecadando as multas que aplicar;

VIII - fiscalizar, autuar e aplicar as penalidades e medidas administrativas cabíveis relativas a infrações por excesso de peso, dimensões e lotação dos veículos, bem como notificar e arrecadar as multas que aplicar;

IX – fiscalizar o cumprimento da norma contida no art. 95, aplicando as penalidades e arrecadando as multas nele previstas;

...;

XIII - integrar-se a outros órgãos e entidades do Sistema Nacional de Trânsito para fins de arrecadação e compensação de multas impostas na área de sua competência, com vistas à unificação do licenciamento, à simplificação e à celeridade das transferências de veículos e de prontuários dos condutores de uma para outra unidade da Federação;

...;

XVII - registrar e licenciar, na forma da legislação, veículos de tração e propulsão humana e de tração animal, fiscalizando, autuando, aplicando penalidades e arrecadando multas decorrentes de infrações; (Redação dada pela Lei nº 13.154, de 2015)

Por todo o exposto, no nosso entendimento, trata-se de um caso típico de indicação de aplicação da tecnologia Blockchain, onde as bases de dados envolvidas demandam requisitos de manutenção descentralizada pelos órgãos fiscalizadores de trânsito Brasileiro, em suas 3 (três) esferas: Federal, Estadual e Municipal, com integração, segurança e confiança entre os entes envolvidos, e ao mesmo tempo, necessidade de consultas recorrentes por todos os órgãos integrantes do SNT, bem como pelos cidadãos habilitados, como premissa básica para consecução de um trânsito em condições seguras como direito de todos.

4 SIMULAÇÃO DE REGISTRO DE ARRECADAÇÃO DE INFRAÇÕES

Dentre as 3 (três) bases de dados, apresentadas no capítulo anterior, optou-se por uma simulação de aplicação da tecnologia Blockchain no processo de manutenção da base de dados RENAINF, a qual hoje é mantida numa arquitetura centralizada pelo DENATRAN, através do SERPRO.

4.1. CONTEXTO ATUAL

Segundo [Pellizzon, 2017], o RENAINF é um sistema de gerenciamento e controle de infrações de trânsito, integrado ao RENAVAM e ao RENACH, e tem por finalidade criar e manter a Base Índice Nacional de Infrações de Trânsito (BINIT) e proporcionar condições operacionais para o registro das mesmas, viabilizando o processamento dos autos de infrações, das ocorrências, bem como o intercâmbio de suas informações. Os órgãos e entidades de trânsito integrantes do RENAINF são classificados em 3 (três) níveis de enquadramento, segundo a abrangência das suas atividades, e respondem pelas atribuições especificadas na Portaria nº 02/2018 [DENATRAN, 2018]:

a) **Departamento Nacional de Trânsito – DENATRAN:** nível I – Órgão Coordenador Geral do RENAINF (OCG);
b) **Órgãos e entidades executivos de trânsito dos Estados e do Distrito Federal:** nível II – Órgão Coordenador Estadual ou Distrital do RENAINF (OCE) ou (OCD), respectivamente;
c) **Órgãos e entidades executivos e rodoviários da União, dos Estados, do Distrito Federal e dos Municípios, com competência para impor penalidade de multa de trânsito:** nível III – Órgão Arrecadador (OA).

Uma vez validada e liquidada, o rateio da arrecadação de multas registradas no RENAINF está definido no Anexo V da Portaria nº 02/2018 do DENATRAN [DENATRAN, 2018], a qual estabelece instruções complementares para a operacionalização do RENAINF. São previstas as seguintes situações de arrecadação, com a respectiva distribuição do valor arrecadado:

a) **Multa arrecadada através da notificação da penalidade emitida pelo órgão autuador:**

- 5% para o DENATRAN, através do Fundo Nacional de Segurança e Educação de Trânsito (FUNSET);

- Restante para o órgão autuador.

b) Multa arrecadada pelos órgãos e entidades executivos de trânsito dos Estados e do Distrito Federal de registro do veículo, aplicada pelos demais órgãos ou entidades integrantes do RENAINF:

- 5% para o DENATRAN, através do Fundo Nacional de Segurança e Educação de Trânsito (FUNSET);

- R$ 6,35 (seis reais e trinta e cinco centavos) para o DENATRAN, sendo R$ 3,00 (três reais) referentes à gestão, administração e prestação de informações e R$ 3,35 (três reais e trinta e cinco centavos) para custeio da infraestrutura de dados e comunicação destinados à circulação e disponibilização das bases de dados RENAINF, RENAVAM e RENACH, que deverá ser recolhido, até o dia 20 do mês seguinte ao da arrecadação da multa à Conta Única do Tesouro através de Guia de Recolhimento da União (GRU), conforme legislação especifica;

- R$ 13,30 (treze reais e trinta centavos) para o órgão arrecadador, sendo R$ 11,00 (onze reais) referentes aos procedimentos operacionais, de sistemas e tarifa bancária para arrecadação da multa e R$ 2,30 (dois reais e trinta centavos) referentes a recebimento e envio das defesas de autuação e de recursos;

- Restante para o órgão autuador.

Todas as rotinas previstas no sistema RENAINF são dependentes da situação de regularidade de habilitação e acesso ao sistema do órgão de trânsito junto ao DENATRAN, com a anuência do Órgão Coordenador (OCE/OCD) a quem se vincula o respectivo órgão. A integração dos órgãos e entidades executivos de trânsito e rodoviário municipais ao Sistema Nacional de Trânsito é normatizada pela Resolução CONTRAN nº 560/2015 [CONTRAN, 2015], que especifica os requisitos e os procedimentos necessários às atividades e competências legais previstas quanto à operação, educação, fiscalização, controle, coleta e análise estatística de trânsito e ainda quanto à engenharia de tráfego e estruturação de Junta Administrativa de Recursos de Infrações (JARI), no mínimo. Para que os municípios passem a fazer parte efetiva do SNT, exercendo plenamente suas funções, precisam criar os seus órgãos ou entidades executivas municipais de trânsito. O manual do sistema RENAINF [SERPRO, 2018] contempla os processos básicos das rotinas de registro, acompanhamento, arrecadação e repasse dos valores das infrações de trânsito, proporcionando, via sistema, a integração dos órgãos e entidades componentes do SNT. O manual do sistema RENAINF

[SERPRO, 2018] descreve 22 (vinte e duas) transações (TR) e 5 (cinco) arquivos gerados pelo sistema, conforme resumo apresentado nas tabelas 4.1 e 4.2 abaixo. Cada transação contempla ou faz parte de um determinado processo, trazendo a informação que é percebida pelo sistema como um comando para realizar uma operação sobre a BINIT.

Tabela 4.1 - Transações do RENAINF.

Transação RENAINF		**Objetivo**
1	401	Consultar uma infração cadastrada na Base Índice Nacional de Infrações de Trânsito – BINIT.
2	402	Consultar infrações para um veículo na BINIT.
3	403	Consultar infrações para um condutor ou proprietário na BINIT.
4	404	Consultar os dados de pagamento registrados para uma infração na BINIT.
5	405	Consultar os dados de ocorrências registrados para uma infração na BINIT.
6	406	Consultar uma conta de órgão autuador cadastrado na Tabela de Órgãos Autuadores do RENAINF.
7	407	Consultar no RENACH o quantitativo de infrações atribuídas ao condutor no período informado.
8	410	Consultar ou propagar os dados de uma transação anteriormente registrada e propagada pela BINIT.
9	411	Registrar uma infração de trânsito no RENAINF, obtendo do RENAVAM a UF de registro e os dados do veículo e de seu possuidor, e do RENACH os dados da habilitação do possuidor.
10	412	Registrar os dados da Notificação de Autuação (NA), e informar os dados do Auto de Infração de Trânsito e da Notificação de Autuação à UF de registro do veículo.
11	413	Registrar os dados da Notificação de Penalidade (NP), recebendo como retorno do RENAVAM os dados recentes do possuidor do veículo.
12	414	Registrar os dados de pagamento de multa ou cancelar o registro indevido de pagamento de multa.
13	415	Informar à nova UF de registro do veículo os dados da infração, do veículo e do possuidor anteriormente registrados no RENAINF.
14	416	Registrar ocorrências relativas às infrações de trânsito.

Transação RENAINF		Objetivo
15	418	Informar o real infrator de uma infração de trânsito.
16	419	Informar à UF do órgão autuador os dados do novo endereço do possuidor quando o veículo for transferido de UF.
17	420	Cancelar o registro de uma infração de trânsito.
18	421	Alterar prazo para interposição de defesa ou prazo de vencimento da notificação de penalidade, e/ou registrar notificação de autuação ou notificação de penalidade por edital.
19	422	Desvincular a infração de trânsito do veículo autuado.
20	430	Registrar os dados de repasse financeiro para o órgão autuador da arrecadação efetuada pela UF de origem do veículo.
21	431	Registrar as infrações correspondentes ao valor repassado para o órgão autuador pela UF de origem do veículo que efetuou a cobrança da multa.
22	432	Registrar, por parte do órgão que arrecadou a multa, a confirmação da realização do repasse financeiro para conhecimento do órgão autuador.

Fonte: (SERPRO, 2018).

Tabela 4.2 - Arquivos do RENAINF.

Arquivo RENAINF	Objetivo
1	Informar a existência de multa de trânsito à UF de habilitação do infrator para registro na base de dados e pontuação.
2	Informar ao órgão de arrecadação, os valores e códigos de barras dos boletos/GRUs gerados pelos órgãos autuadores para repasse dos valores arrecadados.
3	Extrair do RENAINF as informações de registro de pagamentos realizados e não repassados.
4	Cancelar e gerar arquivo periodicamente da base de dados do RENAINF com a informação das infrações sem registro de Notificação de Autuação (NA) por mais de 120 dias.
5	Enviar arquivo contendo as transações pendentes no *restart* (banco de transações não efetivadas).

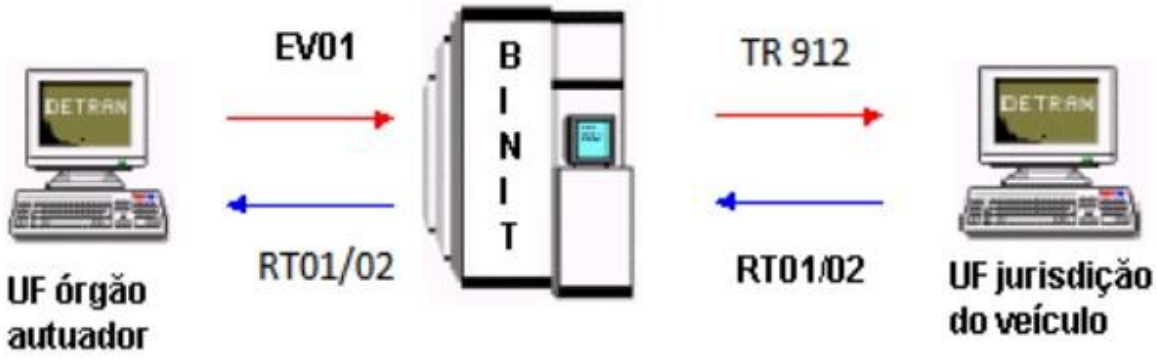
Fonte: (SERPRO, 2018).

De acordo com o manual do RENAINF [SERPRO, 2018], a solução escolhida possibilita que tanto o DETRAN de arrecadação da Infração, quanto o órgão autuador, tenham

um efetivo controle dos repasses financeiros, cabendo ao sistema RENAINF apenas a gestão do fluxo de troca de arquivos. Mensalmente, o próprio órgão autuador ou por delegação o DETRAN da sua Jurisdição, baseado nas regras de rateio do RENAINF, simula o rateio e gera um arquivo, com os dados do boleto bancário ou GRU (para o DNIT ou a PRF) e as informações das infrações computadas no rateio, destinado aos DETRAN que arrecadaram as suas infrações RENAINF. O DETRAN do órgão autuador (ou o DNIT ou a PRF), envia o arquivo de cobrança de repasse ao SERPRO que procede a validação do seu conteúdo, acatando os boletos/GRUs considerados consistentes e rejeitando os inconsistentes. O DETRAN do órgão autuador (ou o DNIT ou a PRF) recebe de volta o seu arquivo com o resultado da validação. Para que cada DETRAN de arrecadação receba apenas um arquivo de cobrança de repasse financeiro por mês, o SERPRO agrupa em novos arquivos de repasse os boletos/GRUs consistentes recebidos dos diversos órgãos autuadores e os envia aos DETRAN de arrecadação para que efetuem o repasse financeiro. O DETRAN de arrecadação após o recolhimento do boleto/GRU emite a transação 432 para informar a realização do repasse ao órgão autuador. Este procedimento substitui as transações 430 e 431. A título de ilustração, e com o intuito de facilitar o entendimento da manutenção da base RENAINF, apresentamos abaixo 7 (sete) procedimentos básicos do sistema, desde o registro de uma infração propriamente dita, até o seu pagamento e consequente rateio:

a) **Registra Infração de Trânsito - TR 411:** tem como objetivo, registrar uma Infração de Trânsito no Sistema RENAINF, que obtém do Sistema RENAVAM a UF de jurisdição do veículo autuado, os dados de identificação do veículo e seu possuidor, e obtém do Sistema RENACH os dados da habilitação do possuidor, se necessário e possível.

Figura 4.1 - Registra Infração de Trânsito.



Fonte: (SERPRO, 2018).

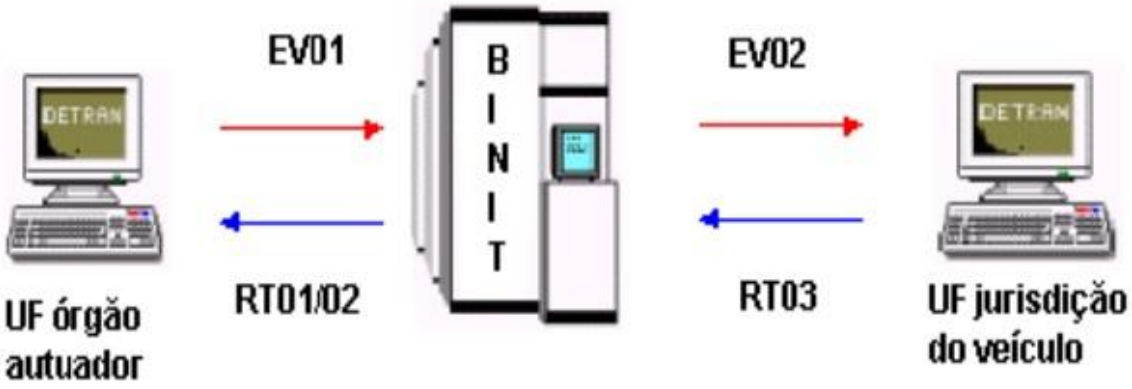
Ao solicitar o registro da Infração de Trânsito, conforme ilustrado na Figura 4.1, a UF do órgão autuador enviará um EV01 (Evento de Transação de Envio 01), com os dados do AIT (Auto de Infração de Trânsito), para a BINIT que validará os dados. Havendo inconsistências, a BINIT retornará à UF do órgão autuador um RT01 (Evento de Transação de Retorno 01) com o código de retorno de execução correspondente. Se a transação for aceita, a BINIT obterá os dados do veículo e seu possuidor à época da infração, de acordo com os dados cadastrados na BIN (Base Índice Nacional) ampliada do Sistema RENAVAM. Identificado o possuidor pessoa física, caso se trate de uma infração de proprietário, ou de uma infração de condutor e não houver condutor indicado no auto de infração, a BINIT obterá os dados de habilitação do possuidor no Sistema RENACH, se houver. A BINIT registrará a infração com os dados da infração e os dados obtidos do Sistema RENAVAM e RENACH, designando um Código RENAINF para essa infração. Após o registro na BINIT, será retornado o RT02 para a UF do órgão autuador. Caso exista mais de uma CNH (Carteira Nacional de Habilitação) para o CPF do possuidor, a BINIT formatará o código retorno da execução da RT02 com o código 249 – *Infração registrada, sem obtenção do CNH do proprietário/arrendatário, devido à existência de mais de um condutor para o mesmo CPF na* BINCO (Base Índice de Condutores).

Durante o processo, a transação efetua as seguintes consistências:

- A UF de origem da transação deve ser a UF do órgão autuador.
- Todos os dados serão consistidos quanto ao formato, à obrigatoriedade e a existência em tabela, quando tabelados;
- Não é permitido o registro de um AIT em duplicidade, ou seja, com a mesma identificação de código do órgão autuador e número do AIT;
- Não é permitido o registro de uma infração de órgão autuador que não esteja atualizado na Tabela de Delegação do Repasse Financeiro;
- As informações de condutor, medição real, medição considerada, limite permitido e unidade de medida deverão corresponder ao código da infração, conforme definido na Tabela de Infrações.

b) **Registra Notificação de Autuação (NA) - TR 412:** tem como objetivo, registrar os dados da Notificação de Autuação de uma Infração de Trânsito, e informar os dados desta Infração de Trânsito e de sua Notificação de Autuação à UF de Jurisdição do Veículo.

Figura 4.2 - Registra Notificação da Autuação.



Fonte: (SERPRO, 2018).

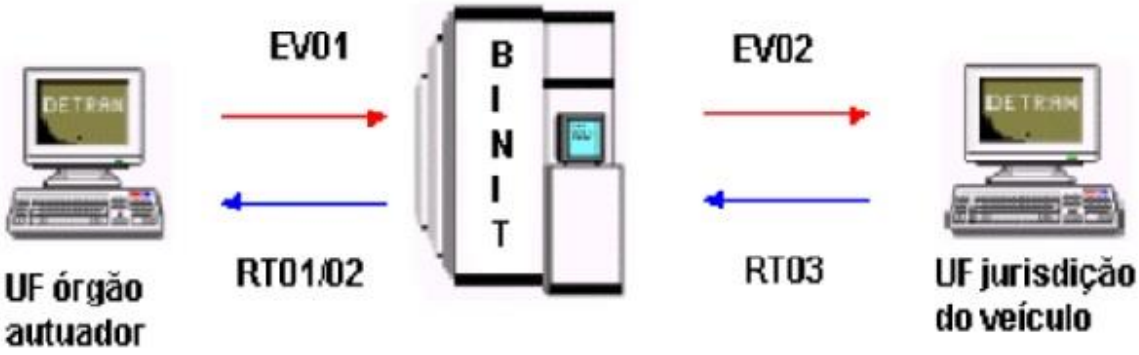
Ao solicitar o registro da Notificação de Autuação de uma Infração de Trânsito, a UF do órgão autuador enviará um EV01 para a BINIT que validará os dados. Havendo inconsistências, a BINIT retornará à UF do órgão autuador um RT01 com o código de retorno de execução correspondente. Se a transação for aceita, a BINIT atualizará os dados da notificação da autuação no registro da infração e retornará um RT02 com código de retorno 000 – *Transação efetuada* para a UF do órgão autuador e acionará o SNE (Sistema de Notificação Eletrônica) para envio de mensagem ao usuário sobre a Notificação de Autuação. A BINIT informará os dados da infração e da notificação à UF de jurisdição do veículo através de um EV02. Por sua vez a UF de jurisdição do veículo confirmará a recepção para a BINIT através de um RT03. Não será gerado o EV02 quando a infração for estadual, ou seja, UF do Órgão Autuador for igual a UF de Jurisdição.

Durante o processo, a transação efetua as seguintes consistências:

- A UF de origem da transação deve ser a UF do órgão autuador;
- Todos os dados serão consistidos quanto à obrigatoriedade e existência em tabela, quando tabelados;
- Não é permitido o registro de uma notificação de autuação em duplicidade;
- A data limite da defesa da autuação deve ser maior ou igual a data de emissão da notificação de autuação.

c) **Registra Notificação de Penalidade (NP) - TR 413:** tem como objetivo, registrar os dados da Notificação de Penalidade de uma Infração de Trânsito, recebendo como retorno dados do possuidor atual no Sistema RENAVAM.

Figura 4.3 - Registra Notificação de Penalidade.



Fonte: (SERPRO, 2018).

Ao solicitar o registro da Notificação de Penalidade da Infração de Trânsito, a UF do órgão autuador enviará um EV01 para a BINIT que validará os dados. Havendo inconsistências, a BINIT retornará à UF do órgão autuador um RT01 com o código de retorno de execução correspondente. Se a transação for aceita, a BINIT atualizará os dados da notificação de penalidade no registro da infração e obterá os dados do possuidor atual do veículo de acordo com os dados cadastrados na BIN ampliada do Sistema RENAVAM, e retornará um RT02 com código de retorno 000 – *Transação efetuada* para a UF do órgão autuador. A BINIT informará os dados da notificação de penalidade à UF de jurisdição do veículo através de um EV02. Por sua vez a UF de jurisdição do veículo confirmará a recepção para a BINIT através de um RT03. Não será gerado o EV02 quando a infração for estadual, ou seja, UF do Órgão Autuador for igual a UF de Jurisdição.

Durante o processo, a transação efetua as seguintes consistências:

- A UF de origem da transação deve ser a UF do órgão autuador;

- Todos os dados serão consistidos quanto à obrigatoriedade e existência em tabela, quando tabelados;

- Não é permitido o registro de uma notificação de penalidade para infração sem notificação da autuação;

- Não é permitido o registro de uma notificação de penalidade para infração com defesa da autuação em julgamento ou defesa da autuação deferida;

- Não é permitido o registro de uma notificação de penalidade de multa para infração com solicitação de penalidade de advertência por escrito em julgamento ou solicitação de penalidade de advertência por escrito deferida;

- Não é permitido o registro de uma notificação de penalidade em duplicidade;

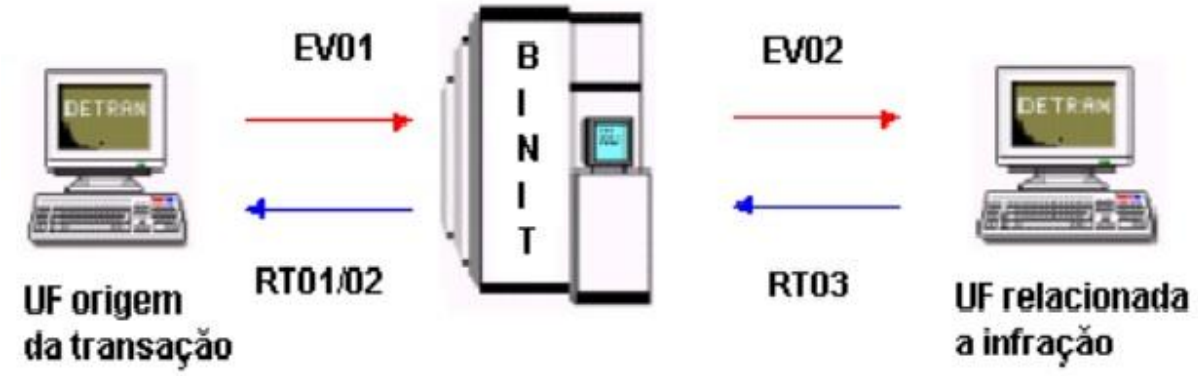
- Não é permitido o registro de uma notificação de penalidade com número de notificação já informado para outra infração de trânsito;

- Não é permitido o registro de uma notificação de penalidade para infração com solicitação de penalidade de advertência por escrito em julgamento (sem resultado);

- Não é permitido o registro de uma notificação de penalidade de advertência por escrito para infração com solicitação de advertência por escrito indeferida.

d) **Registra os dados de pagamento de multa - TR 414:** tem como objetivo, registrar os dados de pagamento de multa por infração de trânsito ou cancelar o registro indevido de pagamento de multa.

Figura 4.4 - Registra os dados de pagamento de multa.



Fonte (SERPRO, 2018).

O registro de pagamento ou cancelamento de registro de pagamento poderá ocorrer por parte da UF do órgão autuador ou da UF de jurisdição do veículo, e deverá ser comandada sempre que for identificado um pagamento. Sempre que houver um pagamento, a UF origem da transação (UF do órgão autuador ou UF de jurisdição do veículo) enviará um EV01 para a BINIT, que validará os dados. Havendo inconsistências, a BINIT retornará à UF origem da transação um RT01 com o código de retorno de execução correspondente. Se a transação for aceita, a BINIT atualizará os dados do pagamento e retornará um RT02 com código de retorno 000 – *Transação efetuada*. Caso a origem da transação seja a UF do órgão autuador, a BINIT informará os dados do pagamento ou cancelamento à UF de jurisdição do veículo, quando

integrada, através de um EV02. A UF de jurisdição do veículo deverá retornar um RT03. Caso a origem da transação seja a UF de jurisdição do veículo, a BINIT informará à UF do órgão autuador que deverá retornar um RT03.

Durante o processo, a transação efetua as seguintes consistências:

- A UF de origem da transação deve ser a UF do órgão autuador ou a UF de jurisdição do veículo;

- Todos os dados serão consistidos quanto à obrigatoriedade e existência em tabela, quando tabelados;

- Os registros de pagamentos pelo DETRAN de jurisdição do veículo só serão aceitos para infrações que tenham o registro da notificação da penalidade, ou seja, o DETRAN de jurisdição do veículo não poderá efetuar o recebimento de uma multa sem que a mesma tenha sido imposta pelo órgão autuador;

- Os registros de pagamento pelo órgão autuador serão aceitos mesmo que não haja registro de notificação de penalidade, bastando que haja o registro da notificação de autuação;

- Todos os pagamentos efetuados devem ser registrados no RENAINF;

- Os pagamentos recebidos a menor pelo agente arrecadador não podem ser registrados e devem ser rejeitados pelo DETRAN de jurisdição do veículo;

- O RENAINF não acatará registro de pagamento com valor diferente do informado pelo órgão autuador no registro da infração, exceto quando o valor informado não ultrapassar R$ 0,5 centavos para mais ou para menos;

- O RENAINF não acatará registro de pagamento com valor com desconto, caso a data de pagamento informada seja maior que a data de vencimento da notificação de penalidade + 5 dias;

- Não serão registradas no RENAINF as devoluções de pagamento efetuadas pelo órgão autuador;

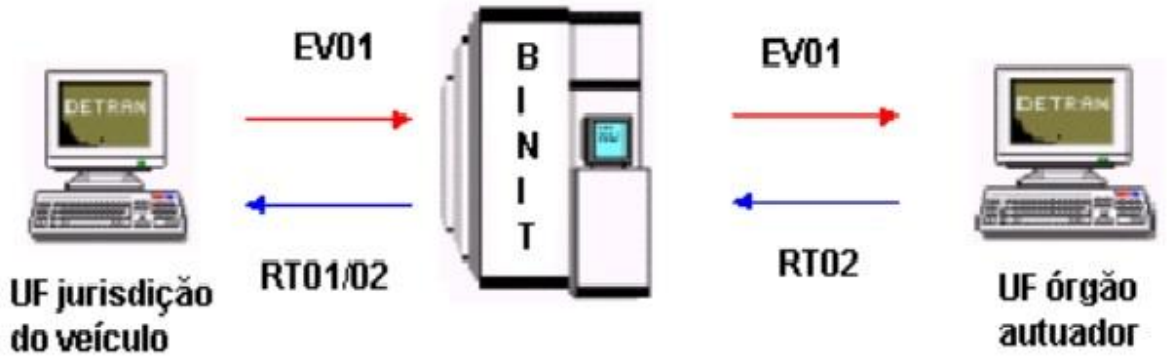
- O cancelamento de registro indevido de pagamento deverá ser utilizado exclusivamente para cancelar o registro por erro, ou seja, para estornar o registro de um pagamento que não ocorreu;

- Para o cancelamento de registro indevido de pagamento deverão ser informados todos os dados do pagamento registrado;

- Não será gerado o EV02 quando a infração for estadual, ou seja, UF do Órgão Autuador for igual a UF de Jurisdição.

e) **Registra Informações de Repasse ao Órgão Autuador: - TR 430:** tem como objetivo, registrar os dados do repasse para o órgão autuador da arrecadação efetuada pela UF de jurisdição do veículo.

Figura 4.5 - Registra Informações de Repasse ao Órgão Autuador.



Fonte: (SERPRO, 2018).

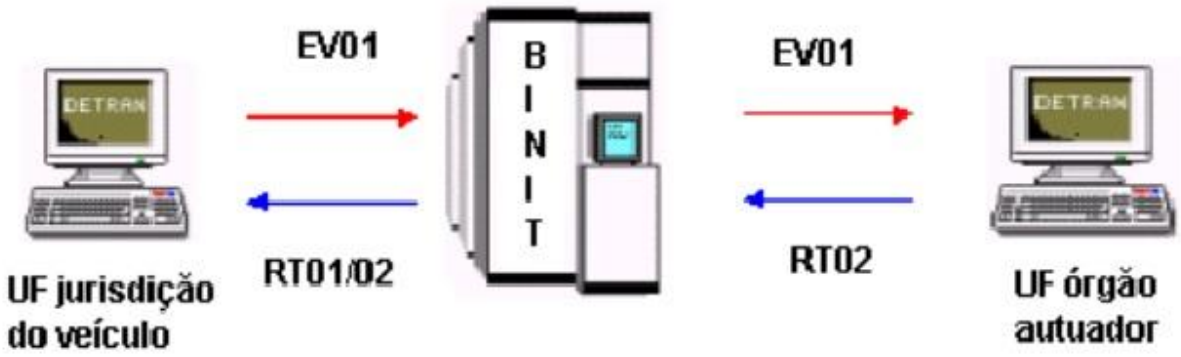
Ao solicitar o registro de informações de repasse ao órgão autuador, a UF origem da transação (UF jurisdição do veículo) enviará um EV01 para a BINIT que validará os dados. Havendo inconsistências, a BINIT retornará à UF origem da transação um RT01 com o código de retorno de execução correspondente. Se a transação for aceita, a BINIT procederá ao registro das informações e retornará um RT02 com código de retorno 000 – *Transação efetuada*. A BINIT informará os dados do repasse de arrecadação à UF do órgão autuador através de um EV01. A UF do órgão autuador deverá retornar um RT02, confirmando que recebeu a informação.

Durante o processo, a transação efetua as seguintes consistências:

- A UF origem da transação deve ser a UF de jurisdição do veículo;
- Todos os dados serão consistidos quanto ao formato, à obrigatoriedade e a existência em tabela, quando tabelados;
- Não é permitido o registro de informação de repasse em duplicidade (com identificador do repasse repetido);
- Não é permitido o registro de repasse com data de repasse posterior a data atual;
- Não é permitido o registro de repasse com quantidade de infrações repassadas igual a zero.

f) **Registra Infrações Repassadas ao Órgão Autuador - TR 431:** tem como objetivo, registrar as infrações correspondentes ao valor repassado para o órgão autuador pela UF de jurisdição do veículo que efetuou a cobrança da multa.

Figura 4.6 - Registra Infrações Repassadas ao Órgão Autuador.



Fonte: (SERPRO, 2018).

Ao solicitar o registro de infrações repassadas ao órgão autuador, a UF origem da transação (UF jurisdição do veículo) enviará um EV01 para a BINIT que validará os dados. Havendo inconsistências, a BINIT retornará à UF origem da transação um RT01 com o código de retorno de execução correspondente. Se a transação for aceita, a BINIT procederá ao registro das informações e retornará um RT02 com código de retorno 000 – *Transação efetuada*. A BINIT informará os dados das infrações repassadas à UF do órgão autuador através de um EV01. A UF do órgão autuador deverá retornar um RT02, confirmando que recebeu a informação.

Durante o processo, a transação efetua as seguintes consistências:

- A UF origem da transação deve ser a UF de jurisdição do veículo;

- Todos os dados serão consistidos quanto ao formato, à obrigatoriedade e a existência em tabela, quando tabelados;

- Não é permitido o registro de infração repassada em um repasse não registrado pela UF de jurisdição do veículo, ou seja, a UF de jurisdição deve registrar previamente o repasse (transação 430), antes de informar as infrações repassadas (transação 431);

- Não é permitido o registro de infração repassada que não esteja cadastrada no RENAINF (código RENAINF não registrado na BINIT);

- Não é permitido o registro de infração repassada que não conste como paga no RENAINF;

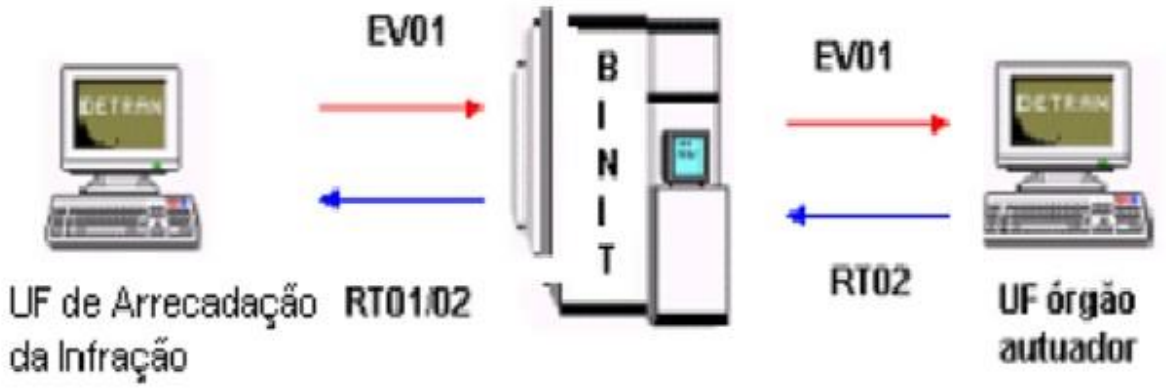
- Não é permitido o registro de repasse de infração em duplicidade;

- Não é permitido o registro de repasse de infração que já tenha sido registrada em outro repasse. Para essa situação será exigida a condicionalidade 2 para aceite do registro;

- Devem ser informados os valores do FUNSET, do DETRAN, do DENATRAN e o valor de repasse ao órgão autuador.

g) **Registra Repasse - TR 432:** tem como objetivo, registrar a confirmação da realização do repasse para conhecimento do órgão autuador pelo órgão arrecadador.

Figura 4.7 - Registra Repasse.



Fonte: (SERPRO, 2018).

Para solicitar o registro da confirmação do repasse ao órgão favorecido (autuador ou o DETRAN, por delegação de competência), a UF origem da transação (UF que arrecadou a infração) enviará um EV01 para a BINIT que validará os dados. Havendo inconsistências, a BINIT retornará à UF origem da transação um RT01 com o código de retorno de execução correspondente. Se a transação for aceita, a BINIT procederá ao registro das informações e retornará um RT02 com código de retorno 000 – *Transação efetuada*. A BINIT informará a confirmação do repasse à UF do órgão favorecido através de um EV01. A UF do órgão favorecido deverá retornar um RT02, confirmando que recebeu a informação. Infração com transação 414 e com suspensão ou cancelamento (via transação 416) pode entrar em um repasse.

Durante o processo, a transação efetua as seguintes consistências:

- A UF origem da transação deve ser a UF que arrecadou a infração;

- Todos os dados serão consistidos quanto ao formato, à obrigatoriedade e a existência em tabela, quando tabelados;

- Não é permitido o registro de confirmação de repasse em duplicidade;

- Não é permitido o registro de repasse com data de repasse posterior a data atual.

Verifica-se portanto, tratar-se de um modelo centralizado, onde os órgãos e entidades de trânsito conectam-se ao RENAINF para registrar infrações e suas ocorrências, nos seus 3 (três) níveis de enquadramento (OCG, OCE/OCD e OA), realizando a leitura e escrita dos seus dados, e que os cidadãos não têm participação ativa no processo de comunicação desenvolvido no âmbito do RENAINF, se restringindo a comunicação por meio de cartas ou mediante protocolo de documentação nos órgãos autuadores componentes do SNT. No final de 2016 o DENATRAN lançou o Sistema de Notificação Eletrônica (SNE) que permite também uma comunicação eletrônica entre o cidadão e os órgãos autuadores que tiverem a adesão já realizada, desde que o usuário opte por essa modalidade, ao baixar o aplicativo no seu dispositivo móvel. Segundo informações obtidas junto aos órgãos que compõem o SNT, com sede no Distrito Federal, DER/DF, DETRAN/DF, DENATRAN, DNIT, PRF e o próprio SERPRO, existem dificuldades de ordem técnica e política na consulta e atualização dessas bases a tempo e hora necessárias, a saber:

- Diversidade de tecnologias envolvidas nos sistemas dos órgãos que compõem o SNT, tanto em nível de software como de hardware, os quais se conectam com as bases de dados do DENATRAN, através do SERPRO, de forma variada (on-line por real time, on-line por rajadas e batch com frequências de atualização não uniformes);

- Infraestrutura de recursos humanos dos órgãos que compõem o SNT, ligados a Tecnologia da Informação, aquém de suas necessidades, resultando em tomadas de decisões baseadas em prioridades que nem sempre são compatíveis com as demandas surgidas. Por exemplo, a disponibilidade de atualização dos sistemas legados, acima citados, em face de alteração dos normativos emanados pelo DENATRAN/CONTRAN;

- Conectividade deficiente entre os órgãos autuadores/arrecadadores e as bases de dados do DENATRAN, tendo em vista que, a infraestrutura de rede dos órgãos que compõem o SNT e os links de comunicações espalhados pelo país, por razões financeiras, técnicas e políticas, não são compatíveis com o tráfego de dados crescente, ficando períodos “off-line”,

trazendo como consequência imediata, a necessidade premente de atualização de seus ativos para atender a demanda.

4.2. MODELO PROPOSTO

Segundo [Drescher, 2018], a decisão sobre a arquitetura a ser implantada em um sistema, pode ser feita de forma independente dos seus aspectos funcionais da camada de aplicação (necessidades do usuário). A arquitetura é apenas um meio de implementação. Cada arquitetura, seja ela centralizada ou distribuída, traz em si vantagens e desvantagens, além do seu modo específico de executar suas tarefas. Sua escolha, traz como consequência os aspectos funcionais e não funcionais de um sistema. Abaixo, apresentamos algumas caraterísticas inerentes ao uso da plataforma de banco de dados tradicional e a tecnologia Blockchain:

a) Banco de dados tradicional

- Centralizado;
- Mutável;
- Baixa transparência (as alterações podem ser feitas via aplicação ou diretamente na base);
- Permite operações CRUD (create, read, update e delete), ou seja, criação, leitura, alteração e exclusão de dados;

b) Blockchain

- Distribuído;
- Imutável (mais segurança);
- Alta transparência (mais credibilidade);
- Permite operações de criação, leitura e validação;
- Extremamente segura.

Conforme citado no item anterior, o processo de manutenção da base de dados RENAINF, a qual hoje é mantida numa arquitetura centralizada pelo DENATRAN, através do SERPRO, tem como principal entrave, as dificuldades de ordem técnica e política na consulta e atualização dessas bases a tempo e hora necessárias. Decorrente disso, uma das maiores dificuldades do modelo atual, reside na obtenção e gestão do rateio dos recursos arrecadados, entre os seus entes responsáveis, em função da relação “órgão autuador x órgão arrecadador”.

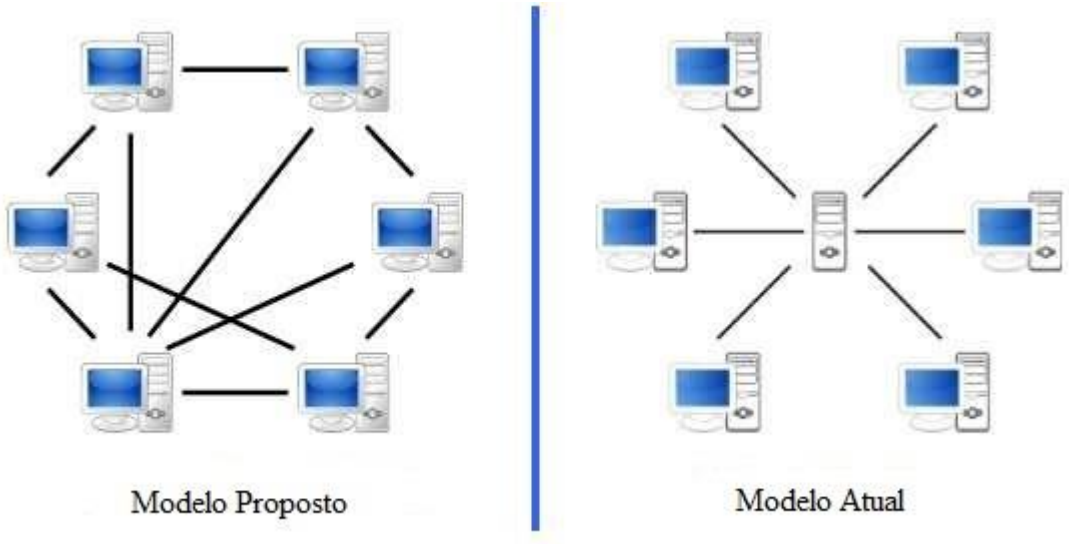
Mensalmente, os órgãos devem proceder a troca de informações, através da permuta de arquivos, entre os seus pares executivos de trânsito e rodoviários partícipes do processo, decorrentes da apuração de suas "contas a pagar" e "contas a receber", em consequência da existência de arrecadações de infrações cometidas dentro e fora da UF de jurisdição do veículo autuado. Outro problema decorrente do não repasse do "contas a pagar" e "contas a receber", reside no fato de que enquanto esta operação não é realizada, não há baixa da infração na base da UF de jurisdição do veículo autuado, fazendo com que o cidadão proprietário do veículo fique impossibilitado de estar regularizado perante o seu órgão executivo de trânsito, em que pese já ter quitado seu débito. Visando mitigar esses entraves, e baseado em todo o arcabouço teórico apresentado no capítulo 2 (Estado da Arte e Revisão da Literatura), propõe-se, aqui, uma mudança de arquitetura e sistemática desse processo, baseada na tecnologia Blockchain, onde não haveria um centro de poder na manutenção e consultas da base de dados do RENAINF, os órgãos participantes estariam conectados entre si e todas as informações estariam distribuídas entre eles, já que cada um possuiria uma cópia de todas as informações dessa base de dados. Além das vantagens já citadas, essa opção tecnológica reduziria sensivelmente as chances de sucesso de um ataque a essa rede, porque ainda que a maioria dos participantes fosse atacada, se restasse apenas um, todas as informações da rede poderiam ser recuperadas por meio dele. Através do modelo ora proposto, se proveria e se manteria a integridade dos dados processados, contemplando as seguintes características básicas:

a) **Arquitetura de rede descentralizada e distribuída baseada em Consórcio:** a solução consistiria numa rede P2P fechada, "com permissão", conforme definido no item 2.4 (Variações de Blockchain), composta pelos órgãos e entidades integrantes do RENAINF (nós da rede), que hoje são cerca de 1.600 (um mil e seiscentos), sob a coordenação do DENATRAN (nó líder), com o propósito de se efetuar o registro compartilhado e seguro das transações distribuídas, onde as partes envolvidas devem assinar as transações entre si, como requisito de consenso dos blocos, para que os mesmos sejam validados, em contraponto com o modelo atual, ou seja, um único provedor (Figura 4.8). Dessa forma, todos os órgãos e entidades de trânsito integrantes do RENAINF fariam parte do sistema e seriam responsáveis pelo seu crescimento, ou seja, quando um registro é adicionado, a integridade da Ledger é verificada por um processo limitado de consenso. Nesta proposta, não há monopólio de informação e/ou de processamento, pois todos os entes que fazem parte da rede tem poder para tal. Esses nós e camadas adicionais, na infraestrutura proposta, teriam, dentre outras

atribuições, a de fornecer um consenso sobre o estado de uma transação a qualquer momento, não havendo a necessidade de troca de arquivos entre eles, como acontece no modelo vigente conforme abordado no item 4.1 (Contexto atual) e ilustrado na tabela 4.2, pois todos esses nós e camadas teriam cópias dos registros autenticados e distribuídos entre eles. Estamos com isso, propondo uma aplicação descentralizada e distribuida, com acesso restrito, cujos participantes não necessariamente confiam uns nos outros, e que, no entanto, exige um registro preciso de todos os eventos que venham a ocorrer. Para sistemas com essas características, ora proposto, [Drescher, 2018] faz as seguintes considerações:

- O número de nós na rede pode variar em razão das falhas técnicas abordadas no item.4.1 (Contexto atual);
- Todo sistema distribuído enfrenta adversidades nas suas redes, deixando a comunicação não confiável no nível das mensagens individuais;
- Nem mesmo um processo de inclusão é capaz de garantir um nível de 100% de confiança entre os nós;
- Até mesmo os nós confiáveis poderão produzir resultados incorretos como consequência de falhas técnicas.

Figura 4.8 - Arquitetura de rede descentralizada e distribuída baseada em Consórcio.



Fonte: (Wikpédia adaptado).

b) Aplicação baseada em Blockchain 2.0: no item 4.1 (Contexto atual) foram ilustradas uma série de transações que são realizadas a partir da ocorrência de determinados eventos inerentes

à manutenção da base de dados RENAINF, como por exemplo o registro, acompanhamento, arrecadação e repasse dos valores das infrações de trânsito entre os agentes autuadores e arrecadadores, proporcionando, via sistema, a integração dos órgãos e entidades componentes do SNT. A aplicação, ora proposta, deverá incorporar os conceitos de contratos inteligentes, característicos da Tecnologia Blockchain 2.0, onde as suas transações seriam processadas por máquinas virtuais implementadas em cada nó da rede, através de *Dapps*, e acessando oráculos externos, como o RENACH e o RENAVAM, para obtenção de dados complementares ao processo. Uma das melhorias de funcionalidades herdadas a partir deste conceito seria o da obtenção a tempo e hora necessários, das "contas a pagar" e "contas a receber" de cada participante da rede, em função da existência de arrecadações de infrações cometidas dentro e fora da UF de jurisdição do veículo autuado. Com esta tecnologia, agrega-se à aplicação não apenas uma renúncia à necessidade de terceiros, como uma autoridade central, mas também garante que todos os participantes da Blockchain conheçam os detalhes do contrato e que os termos contratuais sejam implementados automaticamente quando as condições de requisitos, para tal, forem atendidas. Diferentemente de um contrato tradicional, um contrato inteligente é capaz de obter informações, processá-las e tomar as devidas ações previstas, de acordo com as regras estabelecidas no mesmo. Na prática, esses contratos seriam disparados a partir de eventos comandados pelos sistemas legados de cada integrante da rede. Segundo [Drescher, 2018], aplicações baseadas nesta tecnologia agregam as seguintes vantagens:

- Os contratos inteligentes dispensam intermediários para confirmar as operações, já que a execução é gerenciada automaticamente pela rede e não por pessoas, que na sua essência, são passíveis de erro;
- As informações são criptografadas na Ledger compartilhada, conferindo garantia de transparência, certeza, segurança e legitimidade dos processos automatizados;
- Os contratos inteligentes são criptografados e distribuídos pelos nós da rede, garantido com isso que eles não sejam perdidos ou alterados sem a devida permissão;
- Os contratos inteligentes usam código de software para automatizar tarefas, reduzindo assim tempo em relação aos métodos convencionais;
- Os contratos inteligentes economizam recursos, na medida em que eliminam a necessidade de intermediários no seu processamento;

c) **Independência de sistemas legados:** conforme abordado no item 4.1 (Contexto atual), uma das dificuldades existentes no modelo atual é a diversidade de soluções tecnológicas

existentes e adotadas pelos entes que fazem parte deste processo. A proposta é a de que haja uma aplicação única, baseada na tecnologia Blockchain 2.0, que faça a interconexão entre os sistemas legados dos órgãos e entidades componentes do SNT, na alimentação da base de dados RENAINF. Esta aplicação, a exemplo do SNE, seria provida pelo seu Órgão Coordenador Geral, no caso, o DENATRAN. Desta forma, havendo a garantia de que os órgãos e entidades componentes do SNT, partícipes do processo, se conectem ao sistema proposto, a partir dos seus sistemas legados, teríamos uma maior independência tecnológica das soluções locais;

d) **Confiabilidade e Segurança:** na aplicação proposta, para os entes que compõem a rede, a informação é transparente e verificável, os processos e dados de negócios podem ser compartilhados entre os órgãos e entidades componentes do SNT, o que elimina o desperdício e reduz o risco de fraude, conferindo a ela um grau de confiabilidade expressivo. Os registros da sua base de dados são verificáveis e não são armazenados em um único local. Sua estrutura está calcada em criptografia pesada, usando massivamente chaves públicas e privadas. Seus dados são acessíveis a qualquer nó da rede e a qualquer momento e, como não são centralizados, os seus riscos de segurança são mínimos. Assim, propõe-se uma solução calcada numa tecnologia que lhe confere as seguintes propriedades:

- **Imutável**: o banco de dados não pode ser alterado, revisado ou adulterado, graças a utilização de criptografia, assinatura digital e alto poder computacional distribuído;

- **Somente para concatenação:** é possível se adicionar novos eventos, mas é praticamente impossível alterar dados adicionados anteriormente;

- **Ordenado:** a ordem em que as transações ocorrem é preservada a fim de se obter o mesmo resultado sempre que os seus dados forem agregados;

- **Com timestamp:** o registro da ocorrência de uma determinada transação é válido em qualquer localidade, independente do fuso horário, ou seja, é identificado o momento exato em que algo aconteceu;

- **Aberto e transparente:** ser aberto e transparente é um dos pilares de sustentação da tecnologia Blockchain. É através dessa característica que os seus usuários podem auditar as transações da cadeia;

- **Seguro (identificação, autenticação e autorização):** a solução proposta se baseia em uma rede P2P fechada e "com permissão", restrito aos órgãos e entidades componentes do SNT, exigindo-se identificação e autenticação no seu acesso, além do que, somente o proprietário de sua conta tem autorização para efetuar transações em seu nome;

- **Consistente:** todo nó da rede tem a sua réplica da Ledger, e todas elas são mantidas integras, consistentes e sincronizadas pelos protocolos de consenso inerentes a tecnologia ora proposta. Isto significa que todos os nós da rede precisam reconhecer cada transação para ela se tornar válida.

5 CONSIDERAÇÕES FINAIS

Por todo o exposto no presente trabalho, a tecnologia Blockchain pode ser considerada um divisor de águas, em termos de Segurança da Informação, para determinadas aplicações. Nesta tecnologia, as transações são mais seguras e mais eficazes, se comparadas com sistemas convencionais. Em função disto, é cada vez maior a demanda por plataformas baseadas nesta tecnologia, para garantia de uma maior segurança.

É sabido que, anualmente, organizações no mundo inteiro sofrem diversos prejuízos devido a algum tipo de fraude em seus sistemas. A tecnologia Blockchain pode impedir que essas fraudes ocorram. Em contraponto com os sistemas tradicionais centralizados, nesta tecnologia, o gerenciamento e a autorização de acessos são distribuídos pela rede e, portanto, não há um ponto específico para comprometê-los.

Em geral, as fraudes se baseiam em adulteração, ou mesmo inclusão, de informações sensíveis em bases de dados dentro das organizações. Com a tecnologia Blockchain, a visibilidade da informação é maior, tornando mais fácil a identificação de inconsistências de informações. Nela, os usuários podem acompanhar todo o ciclo de vida dos seus dados, como também, podem ver e relatar o que está acontecendo. Assim, é possível acompanhar todas as alterações feitas nos seus ativos, quem fez e quando foi feito, garantido com isto, a manutenção de sua autenticidade. Não há praticamente nenhuma maneira de se ocultar o que foi feito, mesmo que se tente. Não se trata de uma tecnologia estática que, uma vez desenvolvida permanecerá inalterada, muito pelo contrário, é a base de uma transformação que se descortina, onde a confiança em pessoas ou organizações, será substituída pela lógica infalível da verificação feita por computadores e na eficácia do seu consenso.

Neste sentido, entende-se que esta tecnologia possui aderência quanto a sua aplicação na área governamental e, nesse contexto, vem ao encontro da mitigação dos principais problemas que envolvem a organização e manutenção da base de dados do RENAINF, mantida pelo DENATRAN, conforme preconiza o CTB em seus artigos 19, 20, 21, 22 e 24, a saber:

- **Disponibilidade da informação atualizada em toda a rede através da tecnologia Blockchain:** os dados da blockchain são replicados na rede tão logo haja alguma atualização na sua base. Os seus dados são completos, consistentes, seguros, datados, precisos e amplamente disponíveis;

- **Integridade:** trata-se de uma tecnologia que permite a implementação de registros distribuídos, auditáveis e não fraudáveis;

- **Autenticidade:** mudanças na blockchain são visíveis publicamente por todas as partes envolvidas, criando transparência, e todas as transações são imutáveis, isto é, elas não podem ser alteradas ou deletadas, isto confere à aplicação uma maior transparência;

- **Integração com os sistemas legados**: a tecnologia Blockchain não é excludente, e consegue integrar-se de forma independente com outros sistemas de computação já implantados, não exigindo nenhuma mudança nos seus sistemas atuais;

5.1. TRABALHOS FUTUROS

O presente trabalho procurou evidenciar o potencial de aplicação da tecnologia Blockchain no cotidiano das pessoas. É certo que seu estado da arte carece ainda de um amadurecimento mais consistente, através de um envolvimento mais contundente de seus stakeholders. Sem dúvida nenhuma é um processo que se descortina como algo disruptivo, e que tem atraído o interesse de grandes players de mercado, academia e governos. Não nos é dado o direito de se prever o futuro das coisas, mas a certeza de que quanto mais estudos, pesquisas, aplicações e uso prático envolvendo essa tecnologia, abreviará esse caminho.

Neste diapasão, como sugestão de futuras pesquisas neste tema, relacionadas a área de trânsito, indica-se:

- Ampliação da presente pesquisa à todo o território nacional, envolvendo um maior número de órgãos que compõem o SNT, para que se confirme que a amostragem das informações obtidas junto as entidades envolvidas neste trabalho, refletiu a realidade nacional;

- Ampliação da presente pesquisa, através da inclusão, no seu escopo, do envolvimento do cidadão infrator, como agente pagador, e da rede bancária, como agente arrecadador;

- Ampliação da presente pesquisa, abordando os aspectos relativos a manutenção do Registro Nacional de Carteiras de Habilitação – RENACH, a luz do que preconiza o Código de Trânsito Brasileiro (CTB) em seu artigos 19 (inciso VIII), 140, 147, 159 e 290;

- Ampliação da presente pesquisa, abordando os aspectos relativos a manutenção do Registro Nacional de Veículos Automotores – RENAVAM, a luz do que preconiza o Código de Trânsito Brasileiro (CTB) em seus artigos 19 (inciso IX), 103, 119, 122, 123, 124, 125, 127, 257 e 270;

- Continuidade da presente pesquisa, através do desenvolvimento de um projeto piloto de uma rede descentralizada e distribuída baseada em consorcio, utilizando a tecnologia

Blockchain 2.0, envolvendo os órgãos que compõem o SNT, com sede no Distrito Federal, com vistas a validação prática das propostas aqui apontadas.

6 REFERÊNCIAS BIBLIOGRÁFICAS

AGNER, Marco. **Bitcoin para Programadores**. Instituto de Tecnologia & Sociedade do RIO – ITS. Rio de Janeiro, RJ:2018. Disponível em: https://btcparaprogramadores.marcoagner.org/transacoes.html. Acesso em 07/08/2018.

ANTONOPOULOS Andreas. **Bitcoin security model: trust by computation**. O'REILLY' Radar. 2014. Disponível em: http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html. Acesso em 07/08/2018.

ABREU, Eduardo. **Bitcoin: Um sistema ponto-a-ponto de dinheiro eletrônico**. 2017. Disponível em http://www.embaixadabitcoin.com/wp-content/uploads/2017/11/Bitcoin-White-Paper-Portugues.pdf. Acesso em 25/11/2018.

BRAGA, Alexandre Melo Braga. **Tecnologia Blockchain: Fundamentos, Tecnologias de Segurança e Desenvolvimento de Software**. CPQD 2017. Disponível em https://www.cpqd.com.br/wp-content/uploads/2017/09/whitepaper_blockchain_fundamentos_tecnologias_de_seguranca_e_desenvolvimento_de_softwar_FINAL.pdf. Acesso em 19/07/2018.

CAMPOS, Emília Malgueiro. **Criptomoedas e Blockchain**: O Direito do Mundo Digital. 1ª ed. Rio de Janeiro, RJ: Lumen juris, 2018, 128 p.

CARVALHO, Daniel Balparda de. **Segurança de dados com criptografia**. 2ª ed. Rio de Janeiro, RJ: Book Express, 2001, 218 p.

CARVALHO, Hugo Eiji Tibana. **PKI - Infra-estrutura de Chaves Públicas.** Universidade Federal do Rio de Janeiro. Rio de Janeiro, RJ:2008. Disponível em https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/hugo/index.html. Acesso em 19/07/2018.

COMITÊ GESTOR DE INTERNET NO BRASIL. **Cartilha de Segurança para Internet**, Versão 4.0/CERT.br – São Paulo, SP:2012. Disponível em https://cartilha.cert.br/. Acesso em 19/07/2018.

CEDRO TECHNOLOGIES E BITCOINTOYOU. **Guia: O Que Você Precisa Saber Sobre Blockchain**. 2017. Disponível em: http://blog.cedrotech.com/ebook-sobre-blockchain-o-que-voce-precisa-saber-sobre-tecnologia/. Acesso em 19/07/2018.

CONTRAN. **Resolução nº 560, de 15 de outubro de 2015. Dispõe sobre a integração dos órgãos e entidades executivos de trânsito e rodoviários municipais ao Sistema Nacional de Trânsito – SNT**. Brasilia, DF:2015. Disponível em: http://www.denatran.gov.br/resolucoes.htm. Acesso em 19/07/2018.

DENATRAN. **Portaria nº 02, de 08 de janeiro de 2018. Atualiza as diretrizes quanto ao funcionamento e procedimentos do Sistema de Registro Nacional de Infrações de Trânsito - RENAINF, e dá outras providências.** Brasilia, DF:2018. Disponível em: https://www.denatran.gov.br/images/Portarias/2018/Portaria0022018.pdf Acesso em 19/07/2018.

DRESCHER, Daniel. **Blockchain Básico** Uma introdução não técnica em 25 passos. 1ª ed. São Paulo, SP: Novatec Editora Ltda, 2018, 271 p.

IMPAGLIAZZO, Russell. **One-way functions are essential for complexity based cryptography**. Dept. of Math., California Univ., Berkeley, CA, USA. ISBN 0-8186-1982-1.

LYRA; Joao Guilherme de Miranda et al. **Bitcoin e Blockchain: Aplicações Além da Moeda Virtual**. 2017. Disponível em https://www.blockchainbrasil.org/wp-content/uploads/2017/11/artigoBlockchain.pdf. Acesso em 07/08/2018.

MARTINS; Martins, Pietro. **A tecnologia por trás do bitcoin – Nós desenhamos para você! Clique e entenda!** 2018. Disponível em http://www.bitcoinmove.com.br/a-tecnologia-por-tras-do-bitcoin-nos-desenhamos-para-voce-clique-e-entenda/. Acesso em 07/08/2018.

MILLER, Jaime Núñez. ECDSA. Libro Blockchain, 2017. Disponível em http://libroblockchain.com/ecdsa/. Acesso em 07/08/2018.

MOUGAYAR, William. **Blockchain para negócios** – Promessa, Prática e Aplicação da Nova Tecnologia da Internet. 1ª ed. Rio de Janeiro, RJ: Alta Books Editora, 2017, 224 p.

NAKAMOTO, Satoshi.**Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em https://bitcoin.org/bitcoin.pdf. Acesso em 07/08/2018.

PELLIZZON, J. C. D. **Modelo Conceitual de Sistema de Informação Unificado de Infrações de Trânsito**. 2017, 205 f. Dissertação de Mestrado em Transportes. Departamento de Engenharia Civil e Ambiental da Faculdade de Tecnologia da Universidade de Brasília, 2017.

PIRES, Timoteo Pimenta. **Tecnologia Blockchain e suas Aplicações para Provimento de Transparência em Transações Eletrônicas.** 2016, 57 f. Trabalho de Conclusão de Curso de Graduação em Engenharia de Redes de Comunicação. Faculdade de Tecnologia do Departamento de Engenharia Elétrica da Universidade de Brasília, 2016. Disponível em http://bdm.unb.br/bitstream/10483/16252/1/2016_TimoteoPimentaPires_tcc.pdf. Acesso em 07/08/2018.

RODRIGUES, Elias Italiano. **Estudo sobre Bitcoin: escalabilidade da Blockchain**. 2016. Disponível em http://elias19r.com/files/cv/tcc1-monografia_7987251.pdf. Acesso em 07/08/2018.

SERPRO. **Manual do Registro Nacional de Infrações de Trânsito – RENAINF**, versão 10.2 – Agosto/2018. Serviço Federal de Processamento de Dados. Brasília, DF.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution**: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. 1ª ed. São Paulo, SP: SENAI-SP Editora, 2016, 392 p.