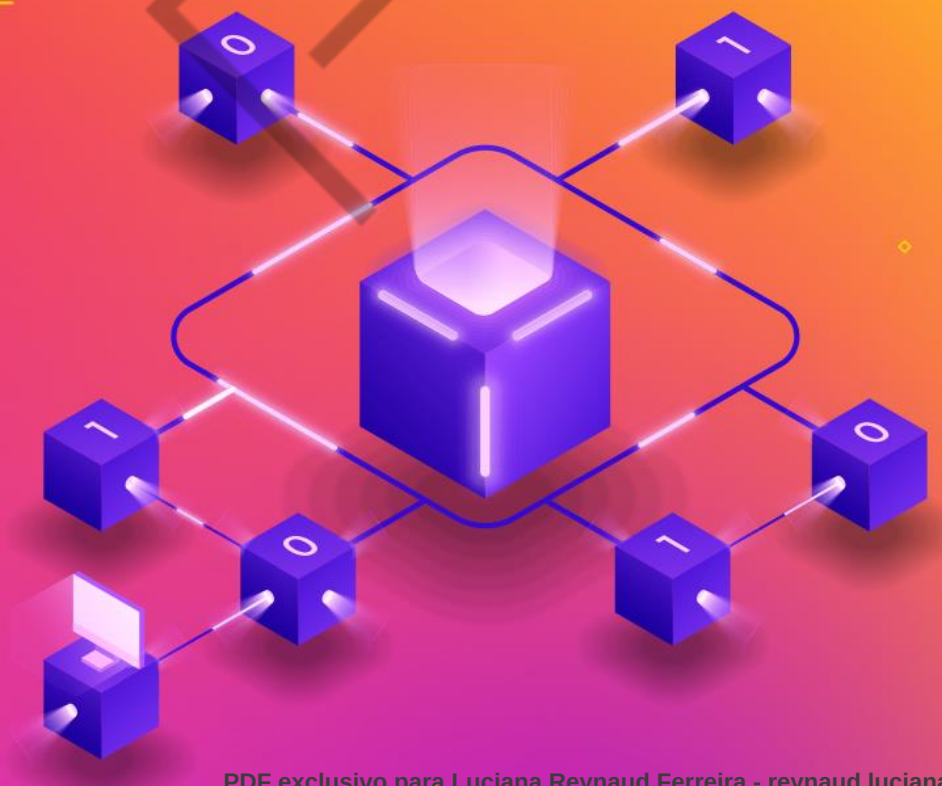
FIAP ON

BLOCKCHAIN ADVANCED

Fundamentação TECNOLÓGICA BLOCKCHAIN

FÁBIO MAÇOLI



2

LISTA DE FIGURAS

Figura 2.1 – Criptografia....4
Figura 2.2 – Sinal de fumaça....5
Figura 2.3 – Bastão de Licurgo....6
Figura 2.4 – Máquina Enigma....6
Figura 2.5 – Criptografia....7
Figura 2.6 – Criptografia simétrica....8
Figura 2.7 – Chave assimétrica....9
Figura 2.8 – Exemplo de função *hash*....10
Figura 2.9 – Certificado Digital....13
Figura 2.10 – Dados do Certificado Digital....13
Figura 2.11 – Assinatura Digital....14
Figura 2.12 – Modelos de estrutura....16

SUMÁRIO

2 FUNDAMENTAÇÃO TECNOLÓGICA BLOCKCHAIN 4
2.1 Criptografia.....4
2.2 Tipos de criptografia.....7
2.2.1 Criptografia de chave simétrica.....8
2.2.2 Criptografia de chave assimétrica 8
2.3 Função *hash*.....10
2.3.1 Função HASH x Blockchain 11
2.4 Certificado Digital 11
2.4.1 Armazenamento do Certificado Digital 12
2.5. Assinatura Digital 13
2.5.1 Conceitos de Assinatura Digital.....14
2.6 Rede P2P 15
REFERÊNCIAS.....17

2 FUNDAMENTAÇÃO TECNOLÓGICA BLOCKCHAIN

2.1 Criptografia

Para darmos início a esta odisseia tecnológica que culmina com o blockchain, e tendo em vista que parte da arquitetura da referida tecnologia encontra-se baseada em segurança e criptografia, é salutar definirmos criptografia e explicarmos um pouco acerca da mesma.

A palavra criptografia tem sua origem no grego, *kryptos* (escondido) e *graphein* (escrita), dessa forma temos como definição que se trata de um conjunto de técnicas que promovem o embaralhamento, ou seja, a codificação das palavras para que elas não permitam sua leitura caso sejam interceptadas, sendo que seus pilares principais são: confidencialidade, integridade, autenticação e não repúdio.

Segundo Bezerra (2010), “A criptologia é a arte ou a ciência de escrever em cifra ou em código”. Em outras palavras, ela abarca o conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir normalmente que apenas o destinatário a decifre e compreenda.

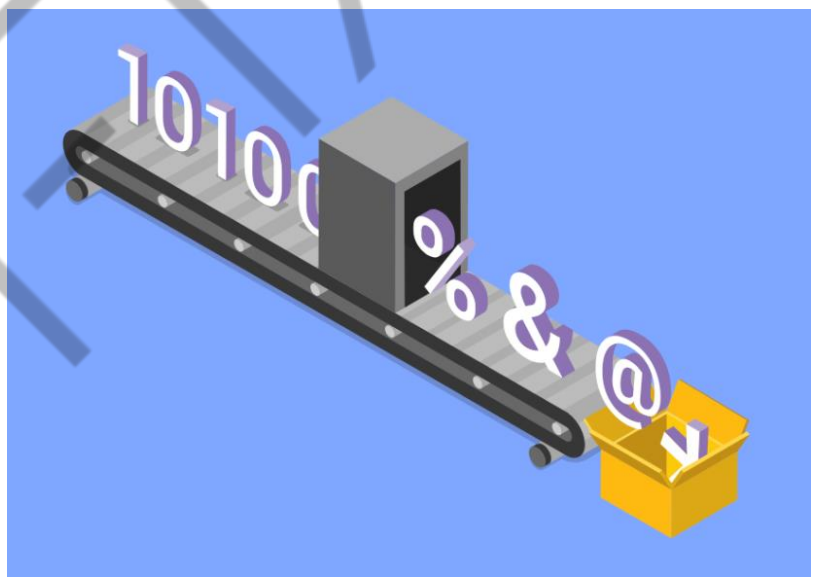


Figura 2.1 – Criptografia
Fonte: CERT.br (2020)

Dessa forma, podemos concluir que a ciência da criptografia consiste em embaralhar mensagens, informações, ou até mesmo inserir códigos entre as mesmas, a fim de tornar a mensagem não compreensível, caso ela seja interceptada

ou lida por uma pessoa que não compreenda seu embaralhamento ou até mesmo os códigos contidos nas informações.

Por meio dos recursos criptográficos, torna-se possível:

- Proteger dados sigilosos.
- Promover o tráfego de mensagens com segurança.
- Guarnecer documentos importantes.
- Manter o sigilo de informações.

Conforme Singh (2003), “A história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de código e os decifradores, uma corrida armamentista intelectual que teve um forte impacto na história humana”.

Figura 2.2 – Sinal de fumaça
Fonte: Humortadela (2017)

O homem sempre teve preocupação em manter e promover o envio de mensagens de forma secreta, seja por interesse político, guerras ou até mesmo manobras a serem feitas envolvendo poder; dessa forma, temos que a utilização da criptografia antecede em muito a era tecnológica, tal necessidade surgiu aproximadamente em 4000 a.C.

Conforme Bezerra, por volta de 500 a.C. foram encontradas cifras hebraicas, mais conhecidas na época como ATBASH, ALBAM e o ATBAH, tais cifras utilizam-se de sistema de substituição simples (monoalfabética).

Já por volta dos anos 450 a.C., os militares gregos faziam uso do bastão de Licurgo ou Scytale. Tratava-se de uma técnica de criptografia que utilizava uma mensagem escrita em uma tira de couro sobre um bastão de largura definida, dessa forma apenas o destinatário que possuía um bastão do mesmo tamanho conseguia ler a mensagem.

Figura 2.3 – Bastão de Licurgo
Fonte: Siriarah (2013)

Assim, podemos concluir que desde o surgimento da humanidade sempre houve a necessidade e o desejo de manter conversas em segurança e com privacidade.

Já na contemporaneidade, mais precisamente durante a Segunda Guerra Mundial (1939-1945), a comunicação entre os alemães no *front* e as embarcações marítimas baseava-se em uma máquina de criptografia denominada Enigma. A referida máquina foi criada pelo alemão Arthur Scherbius, pesava cerca de seis quilos e possuía uma arquitetura considerada simples para os dias de hoje: era constituída por 5 rotores, que eram utilizados com alternância, o que tornava a máquina eficaz na geração criptográfica e no envio de mensagens.

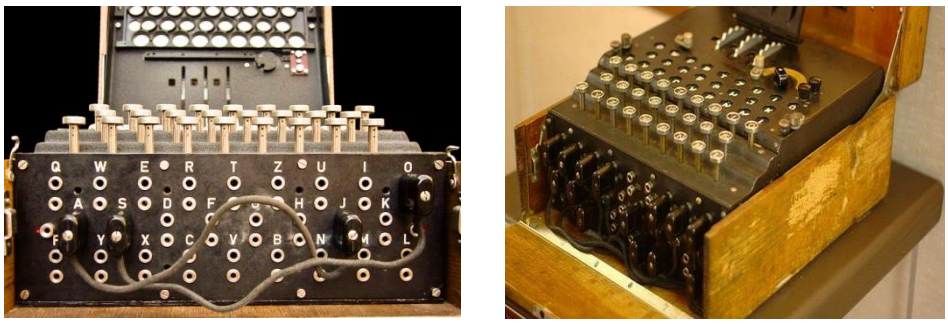


Figura 2.4 – Máquina Enigma
Fonte: Eldiario.es (2014)

Já em 1944, Alan Turing, considerado o pai da computação, inventou a máquina denominada “Bomba”, que permitiu decifrar os códigos gerados pela Enigma e ajudou os Aliados a derrotar a Alemanha.

Dessa forma, podemos concluir que a ciência da criptografia antecede a tecnologia e, com o uso massivo da internet, comunicações de longa distância, transações bancárias, grandes bases de dados, compras on-line, o próprio uso do WhatsApp e toda a demanda tecnológica que está sendo utilizada nos últimos anos, a necessidade crescente e eminente do uso da criptografia para todas essas transações e a garantia da segurança tornou-se fato inerente para suportar tamanha grandeza e capilaridade tecnológica.

Com isso, faz-se hoje o uso da plataforma blockchain, que tem como um de seus principais pilares a segurança e a integridade de dados.

2.2 Tipos de criptografia

Em se tratando de criptografia de dados, atualmente possuímos duas modalidades criptográficas, sendo que as chaves criptográficas estão baseadas em um conjunto de algoritmos que codificam a mensagem, dessa forma mensagens criptografadas só podem ser descriptografadas com o código correto.

Figura 2.5 – Criptografia
Fonte: Crypto Id (2016)

2.2.1 Criptografia de chave simétrica

Também denominada criptografia de chave única, consiste em uma mesma chave para criptografar os dados, ou seja, codificá-los, e utiliza-se da mesma chave para descriptografá-los, ou seja, decodificá-los. Trata-se de um procedimento mais simples de criptografia, por possuir somente uma chave de transação, dessa forma a chave é partilhada entre o emissor e o receptor.

Oferece maior rapidez, simplicidade e, consequentemente, menor segurança.

ALGORITMOS DE CRIPTOGRAFIA DE CHAVE SIMÉTRICA:

RC4

3DES

IDEA

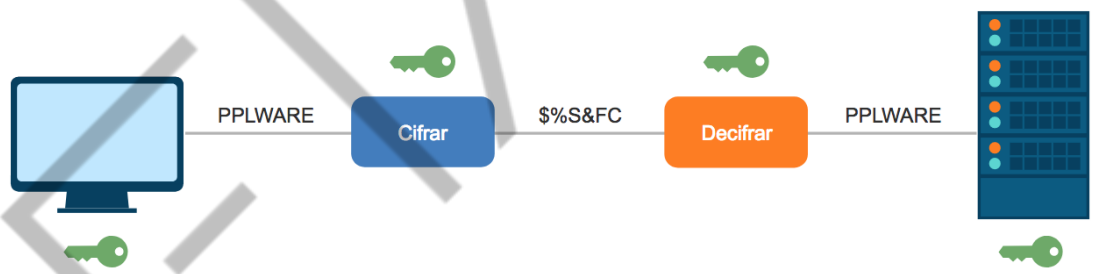


Figura 2.6 – Criptografia simétrica
Fonte: Pplware (2010)

2.2.2 Criptografia de chave assimétrica

Também denominada criptografia de chave pública, para essa transação são utilizadas duas chaves distintas: uma pública, que pode ser divulgada, e outra privada, que é mantida em sigilo pelo seu dono, dessa forma a chave pública é utilizada para codificar, ou seja, criptografar e a chave privada é utilizada para decodificar, ou seja, descriptografar.

Tendo em vista seu mecanismo mais robusto, é um pouco mais lenta, porém implementa maior confiabilidade, garantindo maior segurança no tráfego das informações.

ALGORITMOS DE CRIPTOGRAFIA DE CHAVE ASSIMÉTRICA:

RSA

DAS

ECC

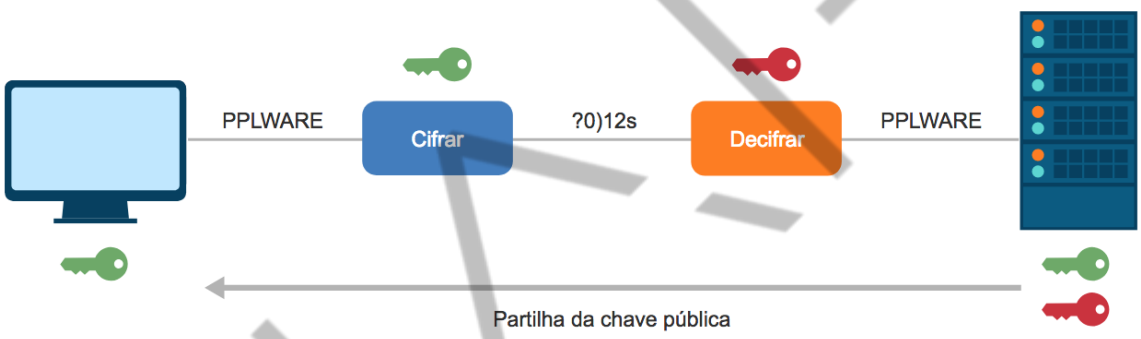


Figura 2.7 – Chave assimétrica
Fonte: Pplware (2010)

IMPORTANTE:

A segurança e a confiabilidade das informações que trafegam na internet, bem como nas ramificações da Tecnologia, tornam-se essenciais nos dias de hoje, em que cada vez mais relações financeiras, compras, vendas e tráfego de informações sigilosas são realizados via internet.

Atualmente, prover a segurança, a integridade e a confidencialidade das informações é fator essencial para o futuro da internet e das tecnologias emergentes.

2.3 Função *hash*

A criptografia *hash* permite que, através de uma *string* de qualquer tamanho, seja calculado um identificador digital de tamanho fixo, chamado de valor *hash*.

O valor *hash* geralmente é formado por 16 bytes (no caso do MD-2, MD-4 e MD-5) ou 20 bytes (no caso do SHA-1), mas pode se estender, embora não passe de 512 bytes.

O conceito teórico do *hash* é a transformação de uma grande quantidade de dados, por meio de um algoritmo matemático, em uma sequência de BiTS, representada em base hexadecimal, garantindo dessa forma a integridade da grande massa de dados, ou seja, é feito um cálculo matemático de uma grande base de dados e atribuído a essa base um número hexadecimal, que, se porventura algum dado dessa base for adulterado, no momento do cálculo do *hash* haverá incompatibilidade, indicando que os dados foram adulterados.

Melhor contextualizando, o *hash* pode ser comparado a um dígito verificador, ou até mesmo a um algoritmo de controle, promovendo um mecanismo que pode assegurar a autenticidade de uma informação ou até mesmo de uma grande massa de informações, garantindo a integridade e a autenticidade das respectivas informações.

EXEMPLOS DE ALGORITMOS DE *HASH*:

MD4 ➔ 128 Bits

MD5 ➔ 128 Bits

SHA-1 ➔ 160 Bits

RIPEMD-160 ➔ 160 Bits

Figura 2.8 – Exemplo de função *hash*
Fonte: Elaborado pelo autor (2020)

Como demonstra a figura Exemplo de função *hash*, um documento elaborado após ser submetido a uma função *hash* irá gerar um número hexadecimal. Esse número é único e, se porventura qualquer caractere do documento original for modificado ao ser submetido à função *hash*, o número será diferente, garantindo a integridade do documento.

2.3.1 Função HASH x Blockchain

Dessa forma, a plataforma Blockchain faz uso da função *hash* em cada bloco processado, e todos os blocos processados e que serão processados se baseiam no *hash* do bloco anterior e assim sucessivamente, fazendo com que a "cadeia de blocos" seja diretamente interligada, garantindo, assim, a total integridade de todas as transações ocorridas no Blockchain, ou seja, se qualquer informação for adulterada em um bloco, irá denunciar o conflito com o *hash* do bloco e dos blocos antecessores e sucessores, criando um link entre blocos, e é justamente todo esse processamento em blocos que garante a confiabilidade do Blockchain.

Mais detalhes acerca de todo o funcionamento e estrutura do Blockchain serão vistos nos capítulos a seguir.

2.4 Certificado Digital

O que é Certificado Digital?

Segundo o site certisign.com.br, o Certificado Digital é a identidade digital da pessoa física e jurídica no meio eletrônico. Ele garante autenticidade, confidencialidade, integridade e não repúdio nas operações que são realizadas por meio dele, atribuindo validade jurídica. Por identificar no meio eletrônico, ele permite que diversos serviços sejam realizados sem a necessidade da presença física, o que significa agilidade nos processos, sustentabilidade e redução de custos.

2.4.1 Armazenamento do Certificado Digital

- Certificado A1 – é emitido e armazenado no computador ou no dispositivo móvel (smartphone ou tablet). Tem validade de 1 ano.
- Certificado A3 – é emitido e armazenado em mídia criptográfica (Cartão ou Token). Tem validade de 1 a 3 anos.

Dessa forma, podemos definir o Certificado Digital como um registro eletrônico constituído por um conjunto de dados que identifica uma entidade, associando uma chave pública à mesma. O Certificado Digital pode ser emitido para uma pessoa, empresas, instituições, equipamentos ou serviços na rede e pode ser comparado a um documento de CPF ou identidade, o qual possui dados pessoais e intransferíveis.

O controle dos Certificados Digitais é feito por uma AC (autoridade certificadora), no Brasil algumas empresas promovem a distribuição e o controle de Certificados Digitais.

DADOS QUE COMPÕEM UM CERTIFICADO DIGITAL:

- Versão e número de série do certificado.
- Identificação do órgão de controle (AC).
- Identificação do dono do certificado.
- Chave pública do dono do certificado.
- Validade do certificado.
- Assinatura Digital.

Figura 2.9 – Certificado Digital
Fonte: DNA Financeiro (2017)

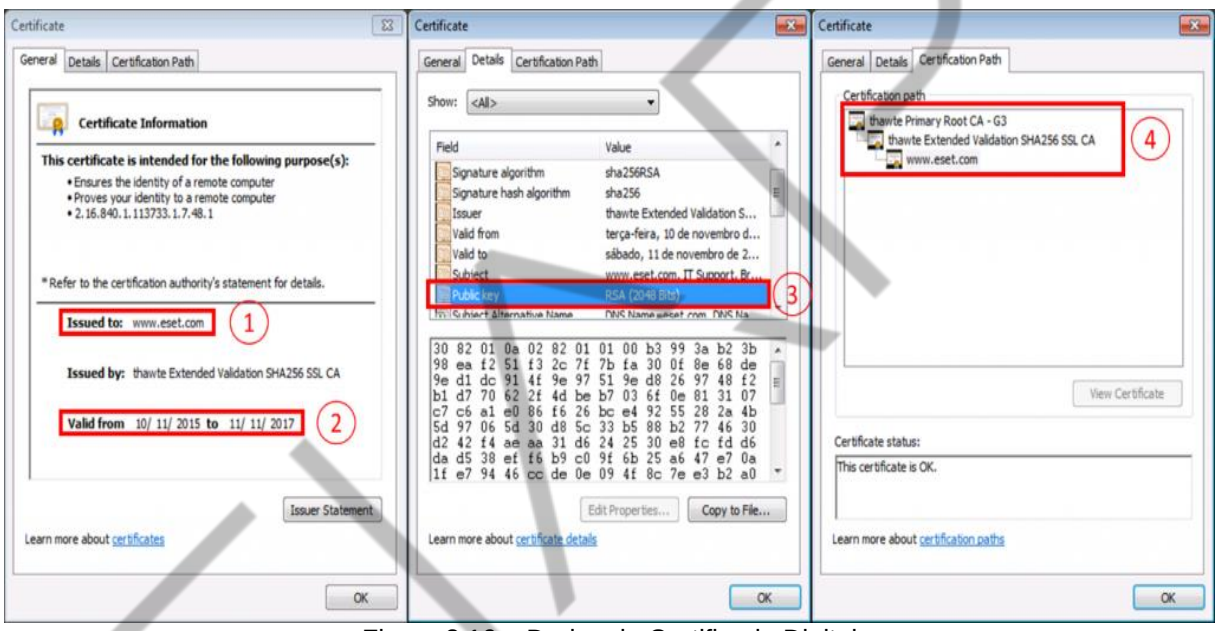


Figura 2.10 – Dados do Certificado Digital
Fonte: We live security (2017)

2.5. Assinatura Digital

Segundo o site QualiSign, a Assinatura Digital, como o próprio nome diz, serve para assinar qualquer documento eletrônico. Tem validade jurídica inquestionável e equivale a uma assinatura de próprio punho. É uma tecnologia que utiliza a criptografia e vincula o certificado digital ao documento eletrônico que está sendo assinado. Assim, dá garantias de integridade e autenticidade.

A validade e a admissibilidade legal da assinatura digital são garantidas pelo artigo 10 da MP nº 2.200-2, que instituiu a Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil, conferindo presunção de veracidade jurídica em relação aos signatários nas declarações constantes dos documentos em forma eletrônica.

Desse modo, temos que assinatura é uma forma eletrônica de validar documentos e transações via internet, tendo em vista a necessidade atual de validar se realmente foi o emissor da transação que a gerou e executou, garantindo assim a autenticidade da transação.

Nos dias de hoje, isso é de suma importância, tendo em vista a quantidade de transações e operações que tramitam via internet, como relações financeiras, contratos etc.

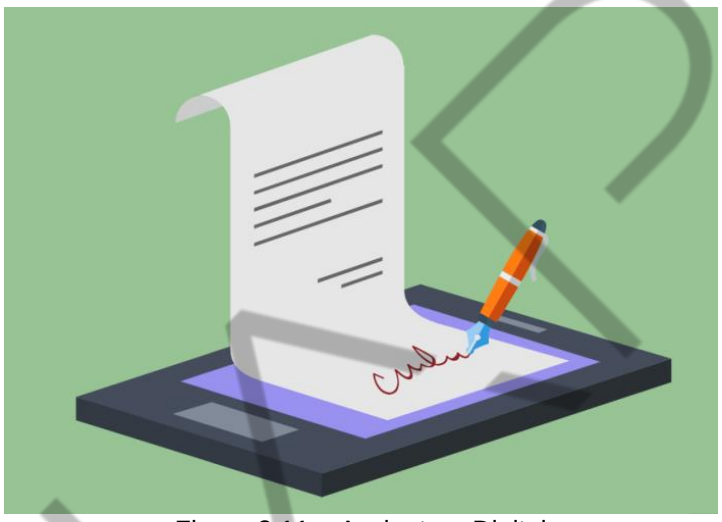


Figura 2.11 – Assinatura Digital
Fonte: Crypto Id (2015)

O conceito da assinatura digital está baseado no fato de apenas o dono da assinatura conhecer sua chave privada, dessa forma, se a mesma foi utilizada para assinar um documento, apenas seu respectivo dono poderia tê-lo feito.

Já a validação e a verificação da respectiva assinatura são feitas pela utilização de uma chave pública, dessa forma, se a assinatura foi codificada com a chave privada, somente uma chave pública correspondente poderá decodificá-la.

2.5.1 Conceitos de Assinatura Digital

Segundo o site QualiSign:

- **Integridade** – Qualquer alteração no documento eletrônico faz com que a assinatura seja invalidada, garantindo assim o princípio da inalterabilidade.

- **Autenticidade** – O autor da assinatura digital utiliza sua chave privada para cifrá-la, de modo a garantir a autoria em um documento eletrônico. Essa autenticidade só é obtida porque a chave privada é acessível exclusivamente por seu proprietário.
- **Não repúdio ou Irretratabilidade** – Quando uma pessoa assina digitalmente, utiliza sua chave privada para cifrar o documento. Assim, ela é impedida de negar a autenticidade da mensagem.
- **Validade Jurídica** – Garantida pelo artigo 10 da MP nº 2.200-2, que instituiu a Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil, conferindo presunção de veracidade jurídica em relação aos signatários nas declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil.

2.6 Rede P2P

É denominada rede P2P, ou rede ponto a ponto, a estrutura de redes de computadores e internet em que não há um servidor definido para armazenamento e compartilhamento das informações, ou seja, todas as estações (computadores) que participam da estrutura exercem o papel de cliente e servidores.

Sua principal função técnica é transmissão e compartilhamento de arquivos em grande escala de forma descentralizada, em que cada estação é denominada um nó da rede. Os dados existentes nesse nó podem ser compartilhados com outros vários nós conectados, sendo que cada nó possui uma parcela de responsabilidade pelos recursos de processamento e tráfego das informações.

Dessa forma, todos os participantes são responsáveis por armazenar e manter a base de dados existente.

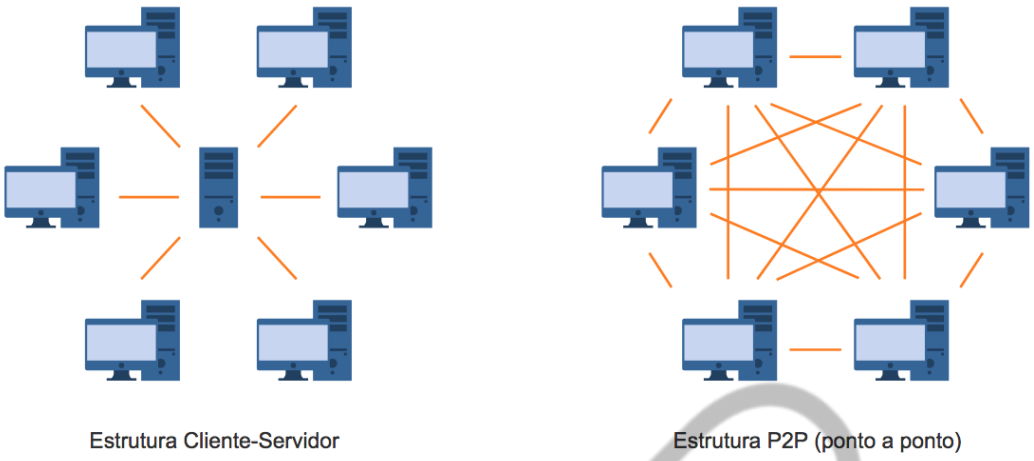


Figura 2.12 – Modelos de estrutura
Fonte: Oficina da Net (2015)

No caso específico da arquitetura Blockchain, isso é muito importante, pois a mesma utiliza-se da estrutura de rede P2P justamente por ser uma tecnologia:

- Descentralizada.
- Compartilhada.
- Com vários nós participando do processamento.
- Distribuída.
- Segura.

Ao longo deste curso será explicado com mais detalhes técnicos como o Blockchain utiliza-se da estrutura de redes P2P, seu funcionamento, características, formas de atualização.

REFERÊNCIAS

BEZERRA, Débora de Jesus; MALAGUTTI, Pedro Luiz; RODRIGUES, Vânia C. da Silva. **Aprendendo criptologia de forma divertida**. Disponível em: <http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf>. Acesso em: 20 jul. 2020.

CERTISIGN. **O que é certificado digital?** Disponível em: <https://www.certisign.com.br/certificado-digital/o-que-e-certificado-digital>. Acesso em: 20 jul. 2020.

MEYER, Maximiliano. **O que é P2P e como ela funciona?** 2015. Disponível em: <https://www.oficinadanet.com.br/post/14046-o-que-e-p2p-e-como-ela-funciona>. Acesso em: 20 jul. 2020.

PINTO, Pedro. **Criptografia simétrica e assimétrica. Sabe a diferença?** 2010. Disponível em: <https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/>. Acesso em: 20 jul. 2020.

QUALISIGN. **Conceito de assinatura digital**. Disponível em: <https://www.documentoeletronico.com.br/assinatura-digital.asp>. Acesso em: 20 jul. 2020.

SINGH, Simon. **O livro dos códigos – a ciência do sigilo**: do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.