# Criptografia: Certificados Digitais

**Carla Santos de Oliveira**[1], **Rafael Sanches Silva**[1],
**Renato Augusto Platz Guimarães Neto**[1],
**Vitor Tavares de Oliveira**[1], **Taynara Cerigueli Dutra**[1]

[1]Instituto Federal do Paraná - Campus Paranavaí (IFPR)
Paranavaí – PR – Brasil

{carlasdeoliveiraf, rafaelsanches.s35}@gmail.com

{renatoplatz11, vitortavares.o55}@gmail.com

taynara.dutra@ifpr.edu.br

Segundo [Bianchetti 2009], criptografia refere-se à escrita codificada, cujo nome deriva de duas palavras gregas: *kryptós*, que significa "escondido" e *gráphein*, "escrita", ou seja, "escrita escondida". Em geral, a criptografia trata da construção e análise de protocolos que impedem a leitura de mensagens por terceiros, e tem como disciplina científica a Criptologia, que estuda os conhecimentos necessários à criptoanálise e à criptografia.

O primeiro uso do termo "criptógrafo" é datado no século XIX, no livro 'O escaravelho de ouro', de Edgar Allan Poe. No entanto, sua origem é, possivelmente, mais antiga, nos hieróglifos irregulares, que foram esculpidos em monumentos no Egito Antigo [Fiarresga 2010], há cerca de 4500 anos. Acredita-se, também, que havia práticas de criptografia clássica na Grécia Antiga, como cifra de transposição *scytale*, utilizada com fins militares em Esparta.

Quando se fala em Criptoanálise Clássica, refere-se à análise de frequência, que é a ferramenta básica para quebrar cifras clássicas. Em outras palavras, determinadas letras do alfabeto aparecem mais frequentemente do que outras; por exemplo, em inglês, "e" é a letra mais comum em toda a amostra dada do texto. Similarmente, o dígrafo "th" é o par mais provável de letras, e assim por diante. A análise de frequência confia numa cifra que não esconde esses padrões de frequência. Por exemplo, numa cifra simples de substituição (em que cada letra é substituída simplesmente por outra), a letra mais frequente numa mensagem cifrada de um texto em português seria a que representa a letra "a". Com a evolução da criptografia, a criptoanálise começou a se automatizar durante as grandes guerras. A primeira vez que a criptoanálise foi aplicada por uma máquina, chamada Colossus, na Segunda Guerra Mundial. Com evolução da criptografia durante a segunda guerra, nasce a Criptoanálise Moderna, que perdura até hoje.

Hoje, uma aplicação frequente da criptografia é no campo de certificados digitais. O certificado digital é a identidade eletrônica de uma pessoa física ou pessoa jurídica [Serasa 2021], com o propósito de ser uma identidade online, responsável por permitir a assinatura de documentos de forma virtual, sem exigir uma assinatura física ou o reconhecimento de firma em cartório, mas com o mesmo valor para a esfera jurídica.

Em certificados digitais, a criptografia segue o mesmo pensamento de qualquer criptografia e seu entendimento é o que permite o entendimento do seu nível de segurança e sua legalidade de uso. Como em toda criptografia, há uma forma de criptografar algo e outra para descriptografar, senão documento ou assinaturas seriam perdidos

[Serasa 2021]. Devido a isso, a criptografia dos certificados funciona como uma chave privada, utilizada para atestar ou restringir acesso pelo emissor, que será a única pessoa autorizada a alterar o seu conteúdo. Na outra ponta, de quem recebe ou acessa o documento, uma chave pública é utilizada, responsável por decodificar a criptografia que atesta a veracidade da informação. Nessa dupla confirmação, há uma comunicação segura e verificada pelo seu transmissor. Com isso, o receptor pode confirmar a autenticidade da informação passada e, se necessário, que ela não será acessada por terceiros.

Há diversos usos para os certificados digitais, como a assinatura digital, o acesso a ambientes restritos e a digitalização de processos e o acesso a eles. Com isso, pode-se entender que, com a tendência de evolução da tecnologia, o uso de certificados tende a aumentar exponencialmente, levando, por consequência, ao aperfeiçoamento das tecnologias relacionadas, em virtude da necessidade de melhores formas de comprovação e segurança sobre ações concluídas ou barradas por tais tecnologias.

Apesar da criptografia ter o propósito de evitar de fraudes, há formas de burlar esse processo, como pela chave de acesso ou por meio de interceptações. Porém, uma nova tecnologia foi proposta em 2008 por [Nakamoto 2008]: a criação do sistema Blockchain para uma moeda virtual, o Bitcoin, que tinha o objetivo de ser virtualmente impossível de ser fraudado. A partir disso, a ideia de proteção contra fraudes começou a ser aplicada a outras moedas, certificações e etc. A proposta é utilizar todos os computadores conectados à rede como estações de criptografia e validação das mesmas, resultando em blocos de validação. Com esse sistema, quanto mais computadores ligados a rede, mais blocos de validação são criados para aumentar sua segurança, ou seja, a segurança aumenta de forma equivalente a quantidade de usuários, como pode ser visto na Figura 1.

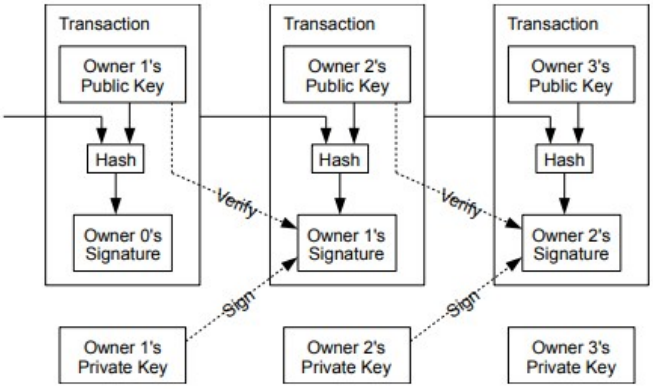


**Figura 1. Representação de uma Blockchain (Fonte: Satoshi Nakamoto [2008]).**

Baseado no que é descrito em [Iconomics 2018], pode-se compreender seu funcionamento a motivação para o seu crescimento rápido nos dias atuais. Isso porque, pela quantidade de computadores na rede, a segurança é virtualmente impossível de ser quebrada. Se cada computador é visto como um bloco, violar a proteção demandaria metade da quantidade de computadores e mais um. Tal resistência a fraudes impulsionou o uso em diferentes áreas virtuais, como no caso das mais recentes NFTs, onde cada imagem divulgada possui um certificado criptografado próprio e integrado a rede, assim, a validade de uma NFT é definida apenas por quem tem este certificado, assim como funciona as assinaturas digitais sem blockchain.

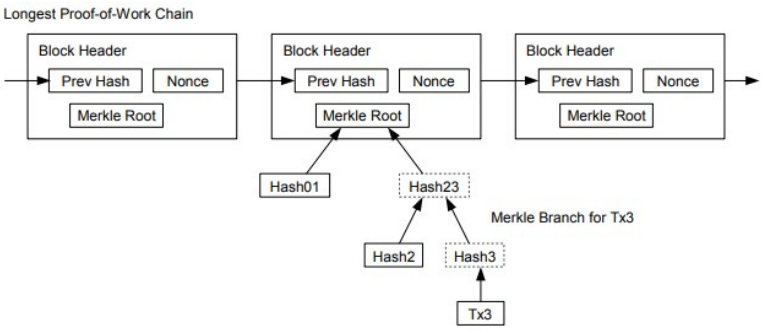


**Figura 2. Representação de uma validação em uma Blockchain (Fonte: Satoshi Nakamoto [2008]).**

Visto o que foi apresentado, pode-se compreender a importância da criptografia ao longo do tempo para a segurança das comunicações, principalmente no atual momento da internet, pela necessidade da certificaão e validação de documentos em âmbito virtual. Dessa forma, a criptografia tornou-se imprescindível para garantir a segurança dos certificados, principalmente com a expansão e melhoria dos usos de Blockchain, que elevam essa segurança contra fraudes a um nível mais elevado, tornando virtualmente impossível a falsificação de certificados e assinaturas.

## Referências

Ahlgren, M. (2022). *50 + Twitter Estatísticas e Fatos para 2022*. Disponível em: https://www.websiterating.com/pt/research/twitter-statistics/. Acessado em 13 de junho de 2022.

Bianchetti, T. (2009). *Criptografia: da história até a aplicação do método RSA*. Disponível em: http://anaisjem.upf.br/download/op-34-bianchetti.pdf.

Fiarresga, V. M. C. (2010). *Criptografia e Matemática*. Disponível em: https://repositorio.ul.pt/handle/10451/3647.

Iconomics (2018). *Como funciona a criptografia na Blockchain*. Disponível em: https://medium.com/eusouelliot/como-funciona-a-criptografia-na-blockchain-cd2cd0b6cde7. Acessado em 13 de junho de 2022.

Machiavelo, A. (2019). *Criptografia e Criptoanálise*. Disponível em: https://rce.casadasciencias.org/rceapp/art/2019/067/.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Serasa (2021). *O que é certificado digital e para que serve ?* Disponível em: https://serasa.certificadodigital.com.br/blog/certificado-digital/o-que-e-certificado-digital-e-para-que-serve/. Acessado em 02 de junho de 2022.

Terada, K. (2008). *Segurança de dados: Criptografia em rede de computador*. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/173353/pdf/0?code=+anKB97zqiojYe/qvz8fFSmeaR/0jQP4J/ACLUkeBlzYf3vt2Xe+ElBwbj/W623BQiuJBAYF0SRX1oI3KjhuQQ==. Acessado em 25 de maio de 2022.