

Projeto em tecnologia *blockchain* em notariação de documentos

A tecnologia *blockchain* é especialmente adequada para processos notariais, na medida em que as suas características asseguram, por desenho, o não repúdio e resistência à adulteração dos dados contidos na mesma.

Existem três áreas em que a *blockchain* pode substituir os serviços notariais, nomeadamente:

- Prova de existência de documento (<https://kctheservant.medium.com/notarization-in-blockchain-part-1-a9795f19e28d>) - A capacidade de certificar a existência de um documento é a base do serviço notarial. A tecnologia *blockchain* assegura, por desenho, que qualquer modificação num documento é detetada, podendo o próprio documento ser guardado na *blockchain* (não aconselhado, devido à potencial privacidade do documento).
A prova de existência pode ser concretizada em dois passos:
 1. Efetuar hash do documento
 2. Guardar essa hash na *blockchain*
- Prova de existência e propriedade de documento (<https://kctheservant.medium.com/notarization-in-blockchain-part-2-1a06d00eb72>) – Nem sempre a prova de existência é suficiente, existindo também a necessidade de saber quem é/são o(s) autore(s) (ou os signatários) do documento.
- Transferência da propriedade do documento (<https://kctheservant.medium.com/notarization-in-blockchain-part-3-ce176c1ac338>) – No ciclo de vida do documento, é ainda necessário prever a transferência da sua propriedade, assim como poder obter os sucessivos donos do documento desde a sua criação.

Os exemplos que são referidos em <https://kctheservant.medium.com/> partem do pressuposto que a tecnologia *blockchain* serve de ajuda à atividade notarial. Neste projeto, o objetivo é desmaterializar as três áreas da atividade notarial referidas acima, de modo a que as mesmas possam ser feitas unicamente com base na tecnologia *blockchain*, sendo possível a uma terceira parte que tenha acesso ao documento validar quando o mesmo foi criado, quem é/são o(s) seu(s) autor(es), quem é/são o(s) seu(s) detentor(es) e quais os donos do documento desde a sua criação (note que na *blockchain* não pode aparecer qualquer informação pessoal, como nome, NIC ou similar).

Neste projeto deverá ser utilizada:

1. Metodologias de desenvolvimento seguro (OWASP, ou outras);
2. Metodologias de teste (OWASP, ou outras);

3. Ferramentas que permitam aquilatar da qualidade do código desenvolvido/utilizado, no que diz respeito a vários factores, como por exemplo: Code Coverage, Abstract Interpretation, Compiler Warnings, Coding Standards, Code Duplication, Security, Dead Code.

Colaboração:

Estes projetos têm a colaboração da Devise Futures, existindo a possibilidade destes projetos poderem evoluir, numa segunda fase, para temas de dissertação de tese de Mestrado.