

Blockchain - Prototipagem rápida de NFTs

Contexto

Os NFTs (*Non Fungible Tokens*) têm uma utilização cada vez maior, estando até a ser utilizados em áreas em que aparentemente não haveria qualquer vantagem na sua utilização, como por exemplo na área postal (e.g., <https://crypto.unstamps.org/>, <https://crypto.post.at/>).

A sua utilização já está standardizada (entre outros, através do ERC-721, assim como do ERC-1155, ERC-998 e do EIP-2309), parecendo também ser usual derivar a chave privada e pública através do BIP39 e BIP32.

Contudo, em relação à plataforma/linguagem a utilizar, assim como em relação à estrutura, custos e usabilidade do NFT (entre outras características), ainda muito há que analisar e avaliar, como por exemplo:

- Ethereum/solidity vs. Flow/Cadence;
- Utilização de Ethereum vs. xDai (ou outra *Ethereum-based sidechain*);
- Base de dados vs. *InterPlanetary File System* (IPFS);
- Optimização da estrutura do NFT, em termos de dados e custos.

Objetivo

Esta dissertação tem como objetivo, entre outros:

- Analisar/avaliar as plataformas NFT existentes, no que diz respeito, entre outros, a custos, usabilidade, facilidade de programação;
- Conceber e implementar uma plataforma para prototipagem rápida de NFTs;
- Utilizar a plataforma concebida para prototipar casos de uso, a decidir durante a dissertação.

Preferência:

Tem-se preferência por candidatos que já tenham tido contacto com NFT, *smart contracts* e Blockchain.

Desenvolvimento da Dissertação de Mestrado

A dissertação de mestrado será desenvolvida nas instalações da Devise Futures, em Braga. Note-se que estão a ser contactadas várias entidades para patrocinarem este desenvolvimento, sendo o trabalho de dissertação remunerado quando isso ocorrer. Caso não exista esse patrocínio, o trabalho da dissertação não será remunerado.

Bibliografia

Identifica-se alguma bibliografia potencialmente relevante:

- ERC-721, Non-Fungible Token Standard
- ERC-1155 Multi Token Standard
- ERC-998 Composable Non-Fungible Token Standard
- EIP-2309: ERC-721 Consecutive Transfer Extension
- BIP39: Mnemonic code for generating deterministic keys
- BIP32: Hierarchical Deterministic Wallets
- Ethereum (<https://ethereum.org/en/>)
- Solidity programming language
- Ethereum sidechain (<https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/sidechains/>)
- Flow primer (<https://www.onflow.org/primer>)
- Introduction to Cadence (<https://docs.onflow.org/cadence/>)

Outra informação importante:

- OpenZeppelin Contracts (<https://github.com/OpenZeppelin/openzeppelin-contracts>)
- NFT storefront (<https://github.com/onflow/nft-storefront>)