

Doggochain — A doggo game blockchain

2nd report

Guilherme Christopher Michaelson Cardoso (14100831)
João Paulo Taylor Ienczak Zanette (14200743)

November 20, 2019

1 Contracts structure

This section will only describe contracts briefly just to clarify **what** they are (i.e. their role in the system). Further explanations of **how** they behave will be cleared in Section 2.

In short, the contracts directly related to Doggochain are structured as follows:

DoggoChain: The main contract, hence responsible for managing database in respect of Players and Doggos, as well as the smart-contract's operations (player challenging, hunting, breeding, etc.). Abstracts player's data as an internal **struct**, since there's no much use for it outside this contract¹.

Doggo: Works as a simple structure for every Doggo's stats, providing an interface that abstract how Doggos evolve (as in stat gaining) and what's their real current stats.

UsageTest: A unit test to check if the system works properly from the point of view of who's going to *use* the API.

Other implementation-specific contracts are designed to compensate some lack of features from Solidity 0.5, e.g. no proper dynamic array handling in storage data. Currently these contracts are:

DoggoList: A simple list data structure implementation, simulated using a mapping from **uint32** to **Doggo** (since there's no generics in Solidity, this implementation must be replicated for every different type) and a **length** variable for element counting.

¹The reason is that the **Player** structure is needed only for players to own their Doggos and mark their existence in the block-chain (i.e. in the game). Every other operation is done considering Doggo-to-Doggo interactions.

OptionalPlayer: Actually not a contract itself, but a structure. Used to compensate the lack of Optional type² in Solidity. Needed since Solidity mappings assume *all* possible keys actually exist and maps to some value (meaning no `hasKey`-related checking), and it does not belong directly to **Player** structure since existence itself is not a player’s property, but rather is a mapping’s constraint.

Apart from that, there are libraries for the more complex operations, so the amount of responsibility in DoggoChain contract’s code becomes reduced:

Battle: For battle simulation. Its only public function is `simulate`, which gives a simulated battle’s results.

Breed: For breeding operations. Its only public function is `breed`, which gives result containing the (possibly) generated Doggo and if the breeding was a success.

2 Function details

This section will be splitted in a subsection for each **main contract and libraries**, since other contracts are merely for implementation details.

2.1 DoggoChain

registerPlayer(string name): Registers a player in the blockchain, making sure the player hasn’t been previously registered, and initializes their list of Doggos.

challenge(address target): Implements the rules for challenging a player for a Player versus Player battle.

breed(Doggo this, Doggo with): This function implements the rules for breeding two Doggos and spawning a new Doggo. The baby will have a combination of the hidden attributes of both parents.

trade(address to, string doggo_name): Implements the rules for trading a Doggo with a specific player.

hunt(doggo): Implements the rules for capturing a wild Doggo and adding it to the player’s collection.

player(address addr): Retrurns the name of the player, and their list of doggos.

totalPlayers(): Returns the number of registered players in the blockchain.

²An “Optional” is a type that handles existence/inexistence of data (without the security/usage issues of using `null`-like value).

So to use any of the game’s features, all the player have to do is to call each function from this contract. Each function will require that the player is correctly registered and will detect that using the `msg.sender` property as player’s address.

For the **challenge**, **trade**, **breed** and **hunt**, the player will be informed of the **results** of that operation via function return data, with computations updating the storage internally. Since they’re related to complex actions, some of their responsibilities are splitted into other libraries (e.g. **Battle** and **Breed**), so these functions will just call the libraries’ ones, get the results and take decisions based on them.

2.2 DoggoList

This is a simple contract that implements a manual array implementation, which is necessary because Solidity doesn’t implement struct copy from memory to storage.

push(Doggo doggo): Inserts a doggo to the end of the list.

pop(): Removes and returns the last doggo in the list.

isEmpty(): Returns true if the list is empty.

2.3 Doggo

Aside from the **DoggoChain** contract (which uses this contract just for storing purposes), some code units such as libraries (e.g. **Battle**) will make extensive use of the **Doggo** contract’s functions. For an example: during simulation in a battle between two Doggos, called “first” and “second” for reference, the library may want to calculate the results of an physical attack action from “first” to “second”. This can be achieved by doing the following:

1. The library calls `first.attack()` and holds its result;
2. Then, the library calls `second.defense()` and also holds its result;
3. Since the attack and defense values means, respectively, how much physical offensive and defensive power a Doggo has, the library can use a formula based to calculate a damage value, i.e. how much “second” will suffer with “first”’s attack.
4. With that damage value calculated, the library will then apply that damage into “second” calling its own function `damage(target, amount)`, passing `second` as argument `target` and the damage value for `amount`.
5. `damage(...)` will, then, decrease the current health points (“HP” for short), i.e. how much that doggo can still keep up with the battle.