Dragonereum

Some headline will be here

October 3, 2018

Version 0.2.10

Abstract

Dragonereum is a cryptocollectible game whereby users can own a dragon, trade their dragons, interbreed them and battle other dragons, collecting rewards and achievements along the way. All of these are done on the blockchain in an open, trusted and decentralized manner.

Our aim is to build the first truly decentralized digital scarcity game, where developers do not have any control over the game once it is deployed. The community will have the ability to verify all the transactions and actions, without the involvement of trusted third parties.

This document discusses the technological and economic implementation of the system. It aims to describe such elements as: random number generation, decentralized breeding algorithm, battle implementation, game mechanics, and a broader economic model which emphasizes the strength of a collectible game built on blockchain.

In this document, we propose the philosophical background, technical foundations and an economic model of Dragonereum, whereby dragon supply is limited by the proposed game mechanics.

Contents

Disclaimer

This whitepaper is provided for informational purposes only, and does not and will not create any legally binding obligation on the authors or on any third party. Therefore, the representations herein should not be relied upon. Dragonereum makes no representations or warranties (whether express or implied), and disclaims all liability arising from any information stated in the whitepaper. This document shall not be considered as a securities prospectus.

No regulatory authority has examined or approved of any of the information set out in this whitepaper. Thus, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

1 Perspective

The appearance of decentralized games defined a new era for digital collectibles: players no longer have to rely on a trusted third party which issues assets in order to preserve the rarity of their belongings, but can fully rely on the autonomous, censorship resistant, trustless and transparent entity - the code of the smart contract.

However, the current offerings lack many important features of the decentralized technology which limits the player's experience to just storing assets securely on the blockchain:

- The scope of actions one can do with his or her items are limited. Most cryptocollectible games function without a game mechanics or a carefully crafted game ecosystem.
- Not properly set supply mechanisms. Unlimited supply reduces the attractiveness of a particular cryptocollectibe.
- The development teams retain full control over the released product and can add new custom-built assets at any time (though within some articulated limits) or even shut down the entire project (https://www.reddit.com/r/CryptoCelebrities/comments/7u4om1/statement_from_developers_read_me/).
- The presale monetization model is widely used thus shifting the developing team's efforts from game development to marketing and PR.
- Additionally, the current solutions still heavily rely upon a centralized infrastructure, which diminishes the advantages of blockchain usage and creates a weak spot and a single point of failure.

We propose a system which is built upon the basics of current technology, with advancements such as rich gamification and an in-game ecosystem with its own in-game cryptocurrency.

The supply of cryptocollectibles is limited by the proposed game design, and, following the game's release, will no longer be under the team's control. Once the game is formally released, the team will relinquish the control of token issue.

An improved free-to-play model is utilized where developers do not collect any fees from players for game assets and the application is built to serve with minimal ties to any servers.

Our long-term goal is to create a fully decentralized game, leveraging all of the unique advantages of the blockchain.

In the following we describe how we aim to achieve those goals. In Section 2 we give an overview of Dragonereum's game ecosystem. In Section 3 we describe the technological limitations faced by Dragonereum and how they are overcome, we outline how we obtain randomness and present the genetics and diversity of our dragon population. Section 4 explains in detail the game mechanics, and how the in-game currency is obtained and distributed. The implementation of the game is described in Section 5, and the possible

platforms with which Dragonereum can be integrated, in Section 6. Lastly in Section 7 and Section 8 the details of the release of the genesis eggs and the Gold allocation are presented correspondingly.

2 Introduction to Dragonereum

Dragonereum is a cryptocollectible, person vs person game whereby users collect and breed unique dragons, engaging in battles along the way.

With our initial version of the decentralized application (dapp), a user will have the possibility to own and manage a dragon or a thunder of dragons. In addition to breeding and battling their dragons, users can buy and sell dragons, collect rewards, compete with other players for in-game achievements and make deals on the game's marketplace.

Each dragon is owned and controlled by a particular address on the Ethereum network. Dragons are securely stored on the blockchain and cannot be modified, replicated or destroyed by any third party.

Every dragon has its unique, immutable set of genes which determines all features and traits of the dragon.

Therefore, a player will have to choose a type of dragon to control (Figure 1), decide on a battle strategy, determine which skills to train with experience earned in battles and how to get better offsprings with further improved *basic skills* (*attack, defense, stamina, speed,* and *intelligence*).

Figure 1: A selection of different types of dragons. Each row represents two varieties of the fire, ice, earth, air, and magic type.

The player's goal might be presented by two paths: a dragon training master or a dragon breeding master. The dragon training master will be an expert in leveling up dragons so he/she can get the strongest dragon and earn in-game rewards as a result of winning battles. The dragon breeding master will know how to interbreed dragons in order to get highly unique and valuable dragons which might be sold on the game's marketplace. Additionally there might be some other unforeseen game paths beneficial to players which will be discovered by them.

The game starts with the purchase of a dragon egg or a dragon from another player or during the initial distribution of genesis eggs. In the case of an egg, a user knows the

egg's parents, but not what kind of dragon will appear from the egg, as this is decided during the egg incubation in accordance with the rules set by Dragonereum's genetics.

After receiving a certain amount of experience and upgrading to the next level, a dragon will be able to either improve its skills or to breed. At that point, the user will have to decide whether to upgrade a dragon's skillset or breed it in order to acquire a new dragon.

Offsprings will rarely outperform their parents right from the hatchery. However, their initial skills (at level 0) would generally be higher than the initial skills of the parent dragons. Therefore, with some training and a few level upgrades, the dragon will eventually outperform its parents.

As in the real world, occasionally there might be a mutation which will cause some of the traits of a new dragon to be much weaker or much stronger than those of its parents. Mutations affect individual genes, so any trait can receive a boost or a skill reset during breeding, but no one will be able to predict which gene will be affected and when.

As going up levels will require even more experience, it will become increasingly difficult to get any dragon's descendants, thus limiting the total population of dragons and avoiding exponential growth.As such, the system is designed to encourage users to be active, and allow them to choose the winning strategy of their own choice.

There are five different dragon types (air, water, earth, fire, and magic). Dragons of different types can interbreed, creating unique offsprings, as can be seen in Figure 2.

Every dragon has the ability to participate in battles. There will be two types of battles: training battles and gladiator battles. Training battles are described below, where they are referred to simply as battles, while gladiator battles will be outlined at the end of this section.

Taking into account the fact that battles are held on-chain they are represented not by a conjoined combat of two dragons but rather by an attack of one active dragon on another passive dragon. When a user wants their dragon to engage in a battle, providing their dragon has enough Health Points (HP), the application offers a choice of dragons of similar Dragon Strength (DS) with which it can battle. The DS is described in detail in Section 4.2. Once a user chooses an opponent, the transaction with the battle is sent to the blockchain. As soon as the transaction is mined and included into the block, the animated battle is shown to the user[1] and the results are displayed.

The attacking dragon always has an advantage as it can adjust its battle tactics according to its opponent's skills. Defending dragons use the default battle tactics defined previously by the owner.All battle results are dependent on the overall skills of the battling dragons, as well as the battle tactics used during the battle.The battle tactics can be defined by

[1]The defending dragon's owner will also have the opportunity to replay the animated battle once they go online

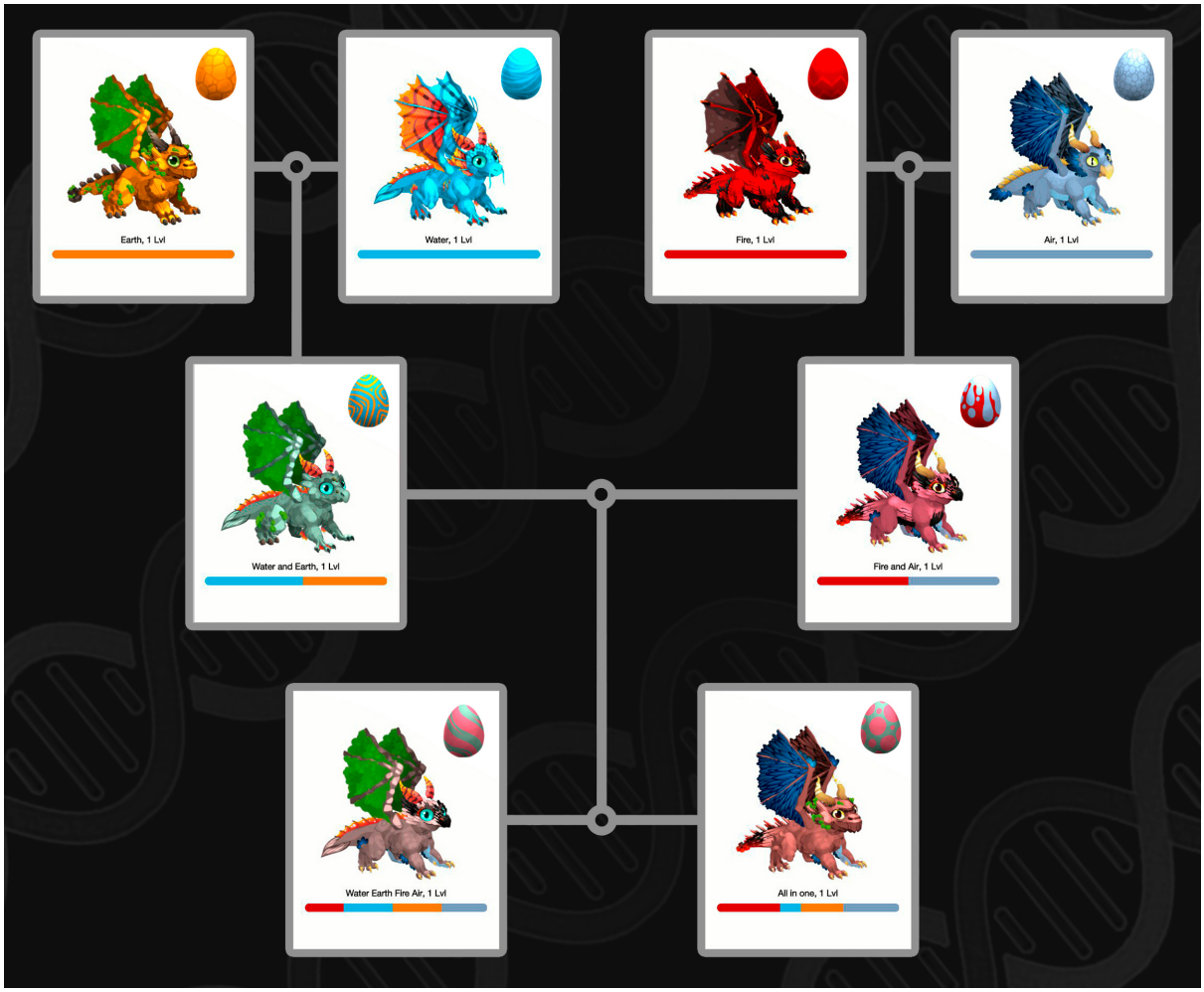

Figure 2: Possible offsprings produced by dragons of different types interbreeding.

two sliders:

- The attack slider selects a value from a range between melee (short-distance attack) and ranged (long-distance attack)
- The action slider selects a value from a range between defense and attack

Every move during a battle is determined by a weighted random number with the value of the weight determined by the positioning of the sliders (for example if the Action Slider is in the position of 20% defense and 80% attack - the dragon will make on average 20% defense moves and 80% attack moves). The dragons with faster speeds always make the first move.

Based on the battle tactics, settings and results of the RNG, dragons are able to:

- Change position
- Attack
- Stand on the defensive
- Use special attack or special defense

Once the faster dragon has made the first move, the opponent has its turn. This continues until the HP for one of the dragons are depleted or the battle exceeds the move limit. If the move limit is exceeded or available gas is depleted but the dragons have an equal amount of HP, the battle result is a draw and both dragons are considered as defeated and no rewards are allocated.

The defeated dragon does not receive any points or bonuses. It only receives a flag protecting it from further attacks, which is valid for one day only.

The higher the intelligence level, the greater the chances of a dragon exploiting its *special attack* or *special defense* skills during the battle.

Special attack or *special defense* is the ability to use the special powers available for each type of dragon. It improves attack or defense during a move. These special moves use Mana.

The results of a battle will be displayed in a rich visual animation, which can be replayed and shared with friends. All users will be able to add comments.

A battle winner receives Experience Points (XP). When the required quantity of XP are earned, the dragon gets a level up and receives some DNA Points (DP), which can be used for breeding or converted into body part level ups and thereby improvements of skills.

Additionally, if the attacking dragon wins, it is credited with Gold as a bonus. Gold is an in-game cryptocurrency which will be distributed to winners from the game's balance. The game's creators will not have any control over Gold stored in the Dragonereum Gold account once it has been deployed to the blockchain.

As Gold has limited availability, the reward for battle winners will decrease over time. The value of the reward will be aligned with the number of dragons in the population and the number of battles held. Once the initial balance in the game's Gold account becomes depleted, the reward adjusts itself according to the sum of fees collected. These are collected for egg incubation and additional in-game features. Consequently, the first players will have an advantage with regards to Gold accumulation.

The only price set by Dragonereum is the amount of Gold required to incubate an egg. This way, Dragonereum controls the number of incubations along with the quantity of new dragons in its overall population.

Gold can also be spent on in-game services (e.g. healing of a dragon after a battle) which will be offered by other players or a system. This will create a platform for social interactions between dragon owners.

Furthermore, as an additional incentive for players to get higher valued dragons and to engage in battles, there will be an internal ranking system, represented by a system of leaderboards, where players can keep track of their achievements and how they score against other dragon owners.

As already mentioned the battles described above are training battles. Those battles allow players to earn XP and Gold from the game account.

Here, we will briefly overview gladiator battles, which are technically the same battles as training battles, but they give players the possibility to place a bet on one of the dragons. They do not let players earn Gold or XP. The simplified process of the gladiator battle can be presented as follows:

- A player decides to offer a dragon on the gladiator arena. He/she offers a dragon together with the amount of ETH he/she would like to place on the battle.
- Other players can offer their dragons for the battle together with their bets.
- The player who initiated the battle confirms one of the offers once the time is up for offers.
- Now other players (every player not necessarily those who participate in this fight) can place bets.
- Once the timer set during the battle initiation has expired, any player can finalize the battle.

3 Technological Overview

3.1 Technology limitations and their implications for the game design

As decentralized technologies are in their early period of development, the game was designed with several limitations in mind.

First of all, the Ethereum network is currently limited to approximately 8M of gas or 15 tx/sec per block. Therefore, we had to limit the dragon population and gas-intensive events (battles, level ups, breeding, incubation, etc.) so that the game's transactions will take just a part of the Ethereum's bandwidth.

This is achieved by offering a limited quantity of genesis eggs and constraining the breeding speed which will limit the supply of new dragons and thus keep the overall game bandwidth within the Ethereum's network capacity.

These initial limitations set a foundation for a broader game economy: supply of in-game currency, cost of incubation, size of a battle reward.

Secondly, as every interaction with smart contracts requires a payment of a miners fee we have to limit the associated mental costs by reducing the number of actions that players have to make and make the code as efficient as possible.

Thirdly, as Ethereum blocks are mined every 15 seconds we have to limit the interactivity of the game mechanics to suit this model.

Additionally, we want to mention that the proposed random number generator (RNG) is in reality a pseudorandom number generator (PRNG) and true randomness is currently unachievable on the blockchain. Therefore, for high value transactions we offer a solution which minimizes the chances of exploiting the game's algorithms.

Lastly, as we rely on Metamask, the current usage is limited to desktop browsers. We will consider moving to mobile once the web platform is operational.

3.2 Obtaining randomness

There are two main approaches used for random number generation. The first relies on some physical phenomenon which is expected to be random. The second relies on a computational algorithm. The latter uses some initial value to generate a random number. However, a generated random number can be reproduced if the initial value (or source of it) and the RNG algorithm is known to the attacker. Hence, this approach, known as pseudorandom, is not truly random.

For some industries (e.g. online gambling), obtaining randomness, or to be more precise pseudorandomness, is a complex issue as the random numbers which influence a game's outcome should be equally unpredictable for all parties.

Within the current online apps, there are multiple ways to obtain randomness, either independently or by relying on third parties. However, users of such apps rarely have the possibility to validate the process of obtaining these random numbers.

On the other hand, for decentralized apps (dapps), where an outcome relies upon the random number, this issue becomes increasingly important due to the limited availability of RNG methods, the price associated with the the use of current solutions and the time required for RNG.

To build a proper decentralized game, where an outcome is defined by a random number, the following specifications of RNG must be met [1]:

1) The RNG can generate a random number in a short period of time, ideally in less than 1 second.
2) The RNG can be trusted and verified by being stored on a blockchain.
3) The RNG should be capable of serving a large number of players simultaneously.
4) A low gas/transaction cost to obtain a random number.

Below we describe several different approaches to obtaining random numbers for Ethereum dapps available today.

3.2.1 Data from blockchain blocks

It is possible to obtain a random (pseudo-random) number from the block data directly, i.e. based on a block number, a block hash, etc. This approach is fast (the random number is generated in the next mined block) and relatively cheap, but there is a possibility that the miners can influence the output of the block in order to affect a generated number. More on this further down.

3.2.2 Use of oracles

This approach is based on some trusted external source of randomness, e.g. www.random.org, which is then delivered to the blockchain by other trusted external sources, e.g. http://www.oraclize.it [2].

This implementation is simple, but its weak spot is that oracles could also be compromised [3]. It also takes longer to obtain a random number as two blockchain transactions are needed. In our tests, it took around 30 seconds to get a random value using this approach.

3.2.3 Commit-reveal

RNG by this method requires two steps. During the first step, participants send hashes of random values and deposit a pledge. During the second step, the sent values are disclosed and a random number is generated based on these initial values [3]. The pledge is required to ensure the faithfulness of the participants. This method is used by RanDAO, Sleth, and Maker-Darts [3].

The disadvantages of this method are that a fee is required for most implementations in order to involve participants for random number generation, and that this method is subject to DDOS attacks. The latter results in a loss of pledges by honest participants [3].

3.2.4 Future blocks

During this RNG, a user sends a transaction that calls the RNG function. The sender's address is added to a list of requests by the RNG smart contract. In the next step, a user requests a random number via another transaction after some blocks have been mined by the network. The required action is taken using a generated random number, based on an initial input and some hashing algorithm, e.g. sha256.

This approach is slower than the other solutions (2 blocks will take about 30 seconds) and the current limitations of the EVM (Ethereum Virtual Machine) allow us to look back only 256 blocks. Hence, a user could just skip a generated number if it does not match his/her expectations.

3.2.5 Signidice algorithm

This approach of RNG is described in Gluk256 repository [3], [4]. The Ethereum smart contract receives a newly generated public key from the owner and awaits a value from the user. After receipt of this value, the owner hashes it with a private key, thus generating a required random number, which might be confirmed by an already published public key.

Regardless of the fact that a centralized application that confirms random numbers is required for this solution, it is still possible to use this method for our use-cases. However, we consider this approach to be too complex for our initial requirements (more on this below).

3.2.6 Dragonereum's solution

The aforementioned algorithm is subject to miner attacks as the timestamp can be manipulated by a miner and several transactions can be included in the block in order to receive the $\_seed$ which matches the desired value.

The timestamp submitted by a miner has to comply with the following rules:

- The timestamp of the current block has to be greater than the timestamp of the parent block
- The timestamp can not be set too far into the future
- The timestamp should not be earlier than when the block was actually mined in order to keep the difficulty as low as possible.

Larger miners can safely manipulate the timestamp for some time without negative consequences. Therefore, we assume that a timestamp can be manipulated by a miner in the range of approximately 10 seconds (the timestamp in the Ethereum blockchain stored in a second format), as constant higher deviation of the timestamp will result in a rejection of the block by other nodes.

Therefore, a malicious miner can have 10 times higher possibilities to manipulate the random number generation outcome. However, the use of the pure implementation of this RNG algorithm is limited in Dragonereum just by the battle transactions.

Low-value transactions

Battle transactions (training battles only) allow players to earn Gold and XP for dragons participating in battles. We assume that these kind of transactions are low-value as each battle rewards users with a limited amount of in-game cryptocurrency and XP which does not have direct monetary value.

Battle transactions can not be compromised by regular players as the RNG includes block.timestamp which is set by a miner. Players can guess what the timestamp will be by looking into historical data and making some assumptions, however it will still be random as it can not be determined in advance with certainty.

Miners on the other hand will have the possibility to alter the timestamp in order to benefit their own battle transactions. However, their possibilities for manipulation are limited by the factors outlined above. Additionally, to gain advantage by manipulating a timestamp the miner will have to do it over a long period of time, which will have a high chance of being noticed by the community. Thus, hurting the goodwill of the company behind it and potentially costing much more in lost profits since part of the miners might potentially leave the mining pool.

Additionally, regular players will be able to win the same amount of Gold (a maximum of 200 GOLD at the initial stage of the game, given the player has a dragon of DS close to the maximum) just by battling dragons of similar DS.

Also, recent developments evidentiated that miners do not easily tend towards manipulation techniques even when a much higher value is at stake [5] . Therefore, we assume that the proposed RNG is sufficient for these use cases.

High-value transactions

There are two types of transactions that we consider to be high-value. Those are:

- Breeding transactions
- Gladiator battle transactions

In the case of high-value transactions an attacker will have a much greater economic motivation to engage in a possible transaction manipulation. For both of these types of transactions we offer certain tweaks to the original algorithm in order to make it more manipulation resistant.

With an original algorithm an attacking miner has a very high chance to clone the required genes (in an ideal situation it is 7/16 or 43.75% for an individual gene and 0.09% ($10 * (7/16 * 9/10)^{10}$) for the whole genome, please refer to Section 3.3). In order to prevent this, we supplemented our RNG algorithm with additional steps in the case of a breeding transaction.

Instead of "direct" breeding, in which case a miner will have an unlimited number of chances to initiate a breeding during a suitable moment, we introduce a Nest - an incubator which holds three eggs, only one egg can be send to the Nest in a block and each forthcoming egg (i) opens the earliest placed egg in the Nest (i-2). Therefore, the Nest always has two eggs in it waiting to be hatched.

A regular player will have the same likelihood of predicting the timestamp that a miner sets for a block, however, now the miner only has a limited amount of time to find a suitable moment to implement the attack, as other miners might include the transaction of someone else sending an egg to the Nest, thus hatching the egg of the attacker.

In the case of gladiator battles - the feature which potentially might store the highest amount of value for the widest array of stakeholders, we offer a variation of the Future blocks approach (see Section 3.2.4). When a gladiator battle is set and an initial timer has run out any player can run the battle at any moment. In the case when the 256 block limit is exceeded, a new timer is set in the future and once it runs out, anyone can start the battle at any time.

This approach allows any interested party to conduct a battle, therefore withdrawing the possibility of waiting for an appropriate moment by those players who will not be happy with the outcome.

The proposed solutions are not ideal and have a degree of vulnerability, however at the current state of decentralized technology and given the use cases, those solutions offer a balance between the simplicity of implementation/usability and the resistance to an attack.

We hope that with the introduction of true randomness in a future development of the Ethereum ecosystem we will be able to switch to more secure algorithms which at the same time will not be more difficult from the player's point of view.

3.3 Blockchain genetics

A major limitation of current non-blockchain games is the process of new character creation. Current solutions allow the user to choose some characteristics of a character or supply a default character with a preconfigured range of abilities. Additionally, all current solutions are centralized by design, so the player does not control or have the ability to verify the process of game character creation, the number of created characters or their set of skills.

As such, the game's creators can, at any moment, release newly created characters with an improved skill set or unique appearance, thus destroying all economic incentives of current players who invested time and money into their characters. This is particularly important for cases where all created characters are collectibles.

We propose a system whereby any third party (even the creators) has no control over new character creation after the release of the system.

To build such a system, all steps of the creation process should be done on blockchain. In order to do that, two main principles must be met:

1) A random number has to be generated on the blockchain or at least stored on the blockchain.

2) Character breeding also has to be done on the blockchain via a publicly accessible smart contract.

RNG was already described in this document and here we will dig into on-chain breeding in the context of its implementation on the EVM.

In Dragonereum, dragon genetics play a crucial role as they determine every aspect of a dragon's character, appearance and fighting abilities. Thus they define the market value of a particular dragon as a cryptocollectible item. As such we attempted to make the genetics of dragons similar to the genetics of real-world animals, nevertheless adding some additional features as we are talking about dragons, aren't we? Additionally, we have to keep the complexity at a level appropriate to EVM.

Also in order to minimize costs, we reduced the complexity of the smart contract to the level where users pay less, but the predictability of breeding is not sacrificed.

We hope that with future releases of new solutions and Ethereum protocols, the cost of breeding will be reduced and we will be able to switch to more advanced forms of breeding algorithms.

In the following text we will describe the breeding algorithm.

Two dragons upgraded to a certain level can breed and produce an egg. This egg can be incubated[2] and a new dragon with the traits of both parents will be born.

[2]The egg is placed in an incubator, once there are five eggs in the incubator, the first egg placed there will hatch, so the addition of the fifth egg in the incubator opens the first egg. The process of hatching continues with the addition of every new egg, out of the eggs inside the incubator, the egg that was in there first hatches everytime a new egg is added.

As can be seen from Dragonereum's egg code (part of a ERC721 token) it stores just the information about parents so the traits of a dragon are determined from this information during the incubation.

```
struct Egg {
       uint256[2] parents;
       uint8 type; // type of a dragon (only for genesis eggs)
   }
```

A hatched dragon on the other hand has much more information stored inside its ERC721 code.

```
struct HealthAndMana {
       uint256 timestamp; // last HP or mana update
       uint32 remainingHealth; // remaining from last update
       uint32 remainingMana;
       uint32 maxHealth;
       uint32 maxMana;
   }
   struct Level {
       uint8 level;
       uint8 experience;
       uint16 points; // upgrade points
   }
   struct Tactics {
       uint8 melee; // melee/range in percentage
       uint8 attack; // attack/defence in percentage
   }
   struct Fights {
       uint16 wins;
       uint16 defeats;
   }
   struct Skills {
       uint32 attack;
       uint32 defence;
       uint32 stamina;
       uint32 speed;
       uint32 intellect;
   }
   struct FightSkill {
       uint8 type; // attack/defence
       uint32 cost; // cost in mana
       uint8 factor;
       uint8 chance; // chance of operation
   }

// classes:   (= types, but it's a reserved word in solidity)
   // 0 - no skill
   // 1 - attack multiplier
   // 2 - defence multiplier
   // 3 - healing

   struct PeacefulSkill {
       uint8 class;
       uint32 cost; // in mana
       uint32 effect; // heal effect or attack/defence buff factor   }
```

```
// types:  // 0 - water
   // 1 - fire
   // 2 - air
   // 3 - earth
   // 4 - magic
   struct Dragon {
       string name;
       uint16 generation;
       uint32 coolness;
       uint256[4] genome;
       uint256[2] parents;
       uint8[11] type; // array of existing types in dragon
       uint256 birth;
   }
```

The genome is stored in an array of 4 numbers of uint256 type, that equals to 128 bytes in total. As it is shown below this is a sufficient size from the diversity perspective.

Dragonereum's dragons have 10 body parts, each consisting of 4 sets of genes, therefore, an example of the whole genome of a dragon will look as follows:

0302841 0400941 0204180 0207320 0105800 **0102291** 0407630 0401391 **0201591** 0306510 0300351 0202210 **0005190** 0305350 0007531 0204551 **0305021** 0004421 0005011 0409360 **0202431** 0107660 0006810 0103420 0202250 **0002831** 0103821 0304430 **0407111** 0107070 0004201 0102570 **0405551** 0303861 0104861 0306670 0200110 **0105031** 0104531 0106750

The order of the body parts is: head, eyes, horns, body, wings, arms, legs, tail, spikes, and skin. The active gene describing the body part in each set of 4 is written in bold type. Each particular body part gives the dragons a boost for a set of *basic skills*. For example, the head is responsible for attack, stamina, and intelligence, while the eyes are responsible for defense, speed, and intelligence (see Section 4.1.1).

The genome sequence determines the appearance and skills of a dragon. Also individual genes from it take part in the breeding process. In this example the first body part is represented by the following code:

0302841 0400941 0204180 0207320

Let's break down the first gene, which is the dominant one in this case, of the first set of genes and see how it influences the appearance of our theoretical dragon:

03 - dragon type (earth dragon)
02 - gene variety (copper dragon)
84 - gene level
1 - dominant

Similar to the natural world, every gene can be recessive (weak) or dominant (strong) and has an influence on the outcome of genome creation during breeding. Every new dragon has two sets of genes (one from each parent) according to the following rules:

- The dominant gene always suppresses the recessive gene.

- A pair of recessive genes will always be transferred to the next generation.

An active gene determines the appearance and skills of a dragon. Active genes are defined by another set of rules:

1) If a pair of genes consists of two dominant genes, the first dominant gene will become the active gene for this dragon.

2) If a pair of genes consists of a dominant and a recessive gene, the dominant gene will become the active gene.

3) If a pair of genes consists of two recessive genes, then the first of the pair will become the active gene.

Therefore, according to rule 1, 0302841 from the example above, is our active gene which determines the appearance of the head as both genes in the first pair are dominant. As can be seen from Figure 3 this dragon will have a Copper dragon's head.

Figure 3: A dragon with an Earth Copper head, whose genome is studied in the text.

Dragonereum's breeding algorithm is represented below.

```
function breeding(
       uint8[16][10] memory _momGenome, // parsed genome
       uint8[16][10] memory _dadGenome, // parsed genome
       uint8 _uglinessChance // if inbreeding
   ) internal returns (uint8[16][10] genome) {
       uint256 _seed = random.random(2**256 - 1);
       uint256 _random;
       uint8 _mutationChance = _uglinessChance == 0 ? MUTATION_CHANCE :
_uglinessChance;
       uint8 _geneType;
       for (uint8 i = 0; i < 10; i++) {
           (_random, _seed) = _getSpecialRandom(_seed, 4); // 0..9999
           genome[i] = _calculateGen(_momGenome[i], _dadGenome[i], (_random %
16).toUint8()); // get 1 random pair from 16 genes pairs
           (_random, _seed) = _getSpecialRandom(_seed, 1); // 0..9
           if (_random < _mutationChance) {
               _geneType = 0;
               if (_uglinessChance == 0) {
                   (_random, _seed) = _getSpecialRandom(_seed, 2); // 0..99
                   _geneType = (_random % 9).add(1).toUint8(); // 1..9
               }
               genome[i] = _mutateGene(genome[i], _geneType);
           }
       }
   }
```

An example of a breeding can be found in our article explaining breeding, mutations and inbreeding effects on dragons [6].

This approach allows us to create a truly trusted world of cryptocollectible dragons, where everyone will be able to observe the breeding process, and no one will be able to influence the results, thus completely removing the necessity of trust as is the case with other solutions available today.

3.4 Dragon diversity

Five different dragon types will be released during Dragonereum's launch. Each type will inherit Regular genes according to the gene variety Table shown in Figure 4. There will be 10000 genesis eggs released during the Genesis. Inbreeding genes and genes of highest quality (Mystery Genes) will play no part in the genesis dragon creation process.

Since every dragon has ten different body parts, each dragon type has 282 475 249 (7^{10}) different dragon varieties. This is not including Inbreeding and Mystery Genes. Therefore, the chance of receiving two similar dragons during Genesis is 0.00070802663492828 7% (1 in 141 237). Consequently, we do not do additional checks for the existence of a particular dragon appearance as chances are very small but this check will require additional gas usage by the smart contract.

Five types of dragons will result in 2 758 547 353 515 625 different breeds when combined. Again, that is without inbreeding and Mystery genes. If all those dragons are to be evenly distributed among the population of the Earth, each person would receive around 360

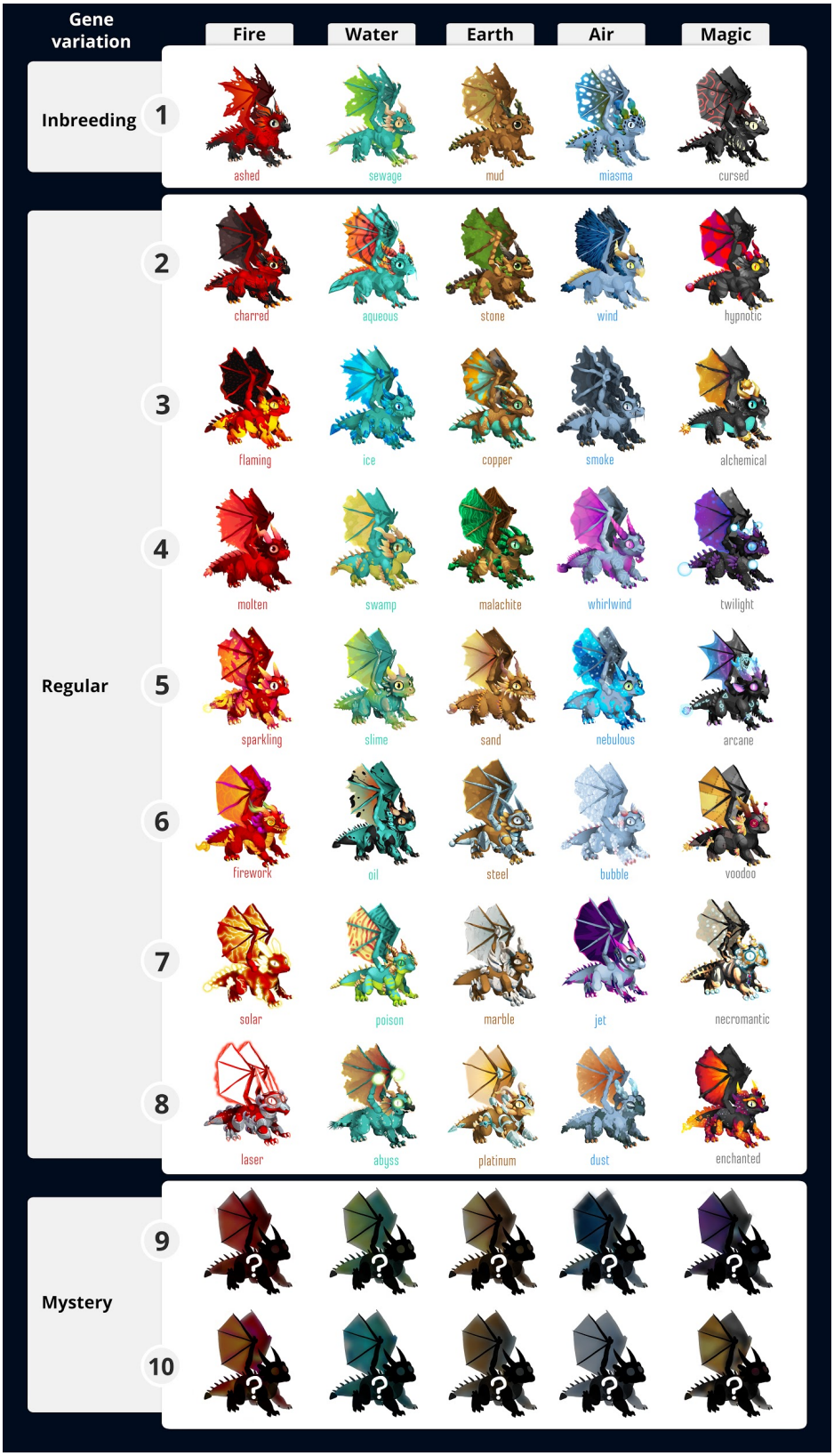

Figure 4: The different dragon types, with all of their possible variations, including inbreeding -row 1, regular rows 2-8, and mystery rows 9, and 10.

000 varieties of dragons.

Together with inbreeding and Mystery Genes, there will be 97 656 250 000 000 000 different dragons originating from those initial five types. This is 12 800 000 for each person in the World.

4 Sustainable Game Ecosystem

Our aim is to create a cryptocollectible game, whereby those users who spend more time playing the game have the possibility to own higher valued dragons and accumulate higher amounts of Gold.

In order to do this the game ecosystem should be balanced and should meet the following criteria:

- The growth of the dragon population should be limited by the game mechanics;
- Early game adopters should have an advantage in accumulating Gold over those players who joined the game at a later date, given that all other comparing factors are on an equal footing.
- There should not be one winning strategy that will allow someone to gain advantage over other players.

In this section we address these issues and explain the solutions that are implemented in order to comply with those requirements.

However, before we do this we have to get a deeper understanding of the game mechanics and underlying math. We have explained some game concepts in Section 2, and here we will dig into the details and formulas.

4.1 Game mechanics

4.1.1 Body parts and basic skills

As it was discussed, there are five Basic Skills: *attack*, *defense*, *stamina*, *speed*, and *intelligence*. The basic skills are calculated based on the dragon's genetics and obtained experience (body parts level ups).

- *Attack* – affects the degree of damage a dragon can cause in a battle.
- *Defense* – measures the ability of a dragon to defend itself during a battle. If the dragon engages in a battle with a dragon which has less *attack*, *defense* determines the damage it can do to the weaker attacking dragon.
- *Stamina* – measures the maximum amount of HP and the speed of regeneration.
- *Speed* – defines which dragon moves first and each dragon's maximum reach.
- *Intelligence* – determines the maximum amount of Mana, along with *speed* for regeneration and the probability of *special attack* or *special defense* being used in battles.

The total skills of a dragon are calculated by summing up all body parts increased by Level Ups. So if you upgrade the wings of a dragon, the total skills of a dragon will also receive a boost.

As it was noted in Section 3.3 each dragon has ten body parts. Each body part is responsible for three particular basic skills and it does not contribute to the remaining two, see Table 1.

	Attack	Defense	Stamina	Speed	Intelligence
Head	✓	×	✓	×	✓
Eyes	×	✓	×	✓	✓
Horns	✓	✓	×	×	✓
Body	✓	✓	✓	×	×
Wings	×	×	✓	✓	✓
Arms	✓	×	✓	✓	×
Legs	×	✓	✓	✓	×
Tail	✓	×	✓	✓	×
Spike	✓	✓	×	×	✓
Pattern	×	✓	×	✓	✓

Table 1: The table shows which body parts are responsible for which particular skills.

4.1.2 Dragon types/families

A dragon might have a combination of body parts of different types and varieties depending on the genome of the particular dragon.

Each dragon type/family is better at a particular basic skill, as shown in Table 2. For example, fire dragons have more *attack* compared to other dragon families.

	Attack	Defense	Stamina	Speed	Intelligence
Fire	1.5	1	1	1	1
Water	1	1	1.5	1	1
Earth	1	1.5	1	1	1
Air	1	1	1	1.5	1
Magic	1	1	1	1	1.5

Table 2: The dragon type factor for each basic skill.

Additionally, every dragon family has a unique advantage over other dragon families, similar to the "rock-paper-scissors" game, as shown in Figure 5. For example, water dragons will generally outperform fire dragons as water puts out fire.

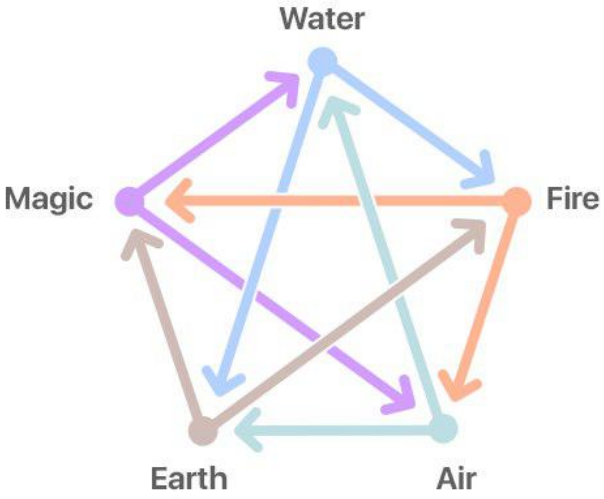

Figure 5: Each dragon family has an advantage over the two dragon families towards which the arrows are pointed: water over earth and fire, fire over air and magic, air over earth and water, earth over magic and fire, and magic over water and air.

Also, each dragon family has a particular *special attack, special defense* and *special peaceful skill.*

4.1.3 Dragon varieties

Each dragon family has genes of different quality. The differences between these varieties influence the dragon's appearance and strength of skills. Therefore, one water dragon might be stronger than another water dragon even without updates or leveling up.

The appearance was already displayed in Figure **??** of Section 3.4, and here we discuss the skills of the different varieties.

Table 3 below provides the dragon variety factors for the five basic skills depending on the different dragon varieties

In Table 3, the first row shows the dragon variety factor for inbreeding dragons, as such it is penalized by our genetics algorithm to be 0.5.

The genes of the highest quality (9–10 in Table 3 above) are Mystery Genes and will only be accessible as a result of mutations. Genesis dragons will not have these genes at all (more on it in Section 7).

The chance for a regular mutation to occur (excluding the case when two relatives inter-

Variety	Codename	Attack	Defense	Stamina	Speed	Intelligence
1 (inbreeding)	Inbreeding	0.5	0.5	0.5	0.5	0.5
2 (regular)	Common 0	1.5	1.5	1	1	1
3 (regular)	Common 1	1	1.5	1.5	1	1
4 (regular)	Common 2	1	1	1.5	1.5	1
5 (regular)	Common 3	1	1	1	1.5	1.5
6 (regular)	Rare 0	2	2	2	1	1
7 (regular)	Rare 1	1	2	2	2	1
8 (regular)	Rare 2	1	1	2	2	2
9 (mystery)	Epic 0	4	4	4	1	1
10 (mystery)	Epic 1	1	1	4	4	4

Table 3: The dragon variety factors for each basic skills depending on the dragon gene variation.

breed) can be described as follows:

- During the incubation there is a 10% probability for each gene to mutate.
- The mutated gene might be of any of the varieties between 2 (regular) and 10 (mystery) listed in column 1 of Table 3 with an equal probability (the 1 (Inbreeding) variety is received only in the case when close relatives interbreed).

Details of inbreeding penalties and chances are described in our medium articles (https://medium.com/@dragonereum).

If a player chooses to inbreed close relatives there is a high probability for a negative mutation will occur. This probability depends on different cases and is:

- Very high for inbreeding full siblings (80%)
- High for inbreeding half-siblings (70%)
- 50% for second and third cousins. The chances of negative mutations might increase if these dragons have several close relatives.

4.1.4 Calculating the overall basic skills of a dragon

The overall skills of a dragon will be calculated as the sum of skills for all its body parts:

$$Sk(j) = \sum_{i=1}^{10} bp^i(j) * f_{dt}^i(j) * f_{dv}^i(j) * L^i, \tag{1}$$

where $Sk(j)$ is one of the five *basic skills*, bp is the body part influence on the particular skill as shown in Table 1, a checkmark corresponds to $bp = 1$ and a cross corresponds to $bp = 0$, f_{dt} is the dragon type factor shown in Table 2, f_{dv} is the dragon variety factor in Table 3 and L is the body part level[3]. The index j denotes the basic skill, $j \in$ *attack, defense, stamina, speed, intelligence* , and the summation index i in the superscript, denotes the body part, $i \in$ head, eyes, horns, body, wings, arms, legs, tail, spike, pattern. The following notation for the basic skill will also be used through the text: Sk(attack)≡A, Sk(defense)≡D, Sk(stamina)≡S, Sk(speed)≡V, Sk(intelligence)≡I.

This can be illustrated by the following example in Table 4. The numbers in the last column will be added to the other body parts and the result will show the dragon's aptitude for in the different basic skills.

	Skill	Body part influence	Dragon type factor	Dragon variety factor	Body part level	
Ashen Legs 3 lvl		Leg	Fire	Inbreeding	3	Total
	Attack	0	1.5	0.5	3	0
	Defense	1	1	0.5	3	1.5
	Stamina	1	1	0.5	3	1.5
	Speed	1	1	0.5	3	1.5
	Intelligence	0	1	0.5	3	0

Table 4: An example, illustrating the calculation of the basic skill for a specific body part - the Legs of a particular dragon.

The maximum available health and mana points are calculated in Equation 2 and 3.

$$H = 5 \times S, \tag{2}$$

$$M = 5 \times I, \tag{3}$$

The current levels of health and mana points available to a dragon might be lower than the maximum calculated in Equation 2 and 3, as a result of a battle, in which the Mana could have been used to activate the *special attack* or *special defense* skills, while the HP could be lost as a result of damage done by an opponent. Mana and HP restore automatically over time.

[3]The body part level is the level of the active gene for each body part.

4.1.5 Dragon Skillfulness Index

In order to represent the dragon skillset in an easier way we offer an aggregative parameter called the Dragon Skillfulness Index. The Dragon Skillfulness Index will be displayed next to the dragon's name, Figure 6.

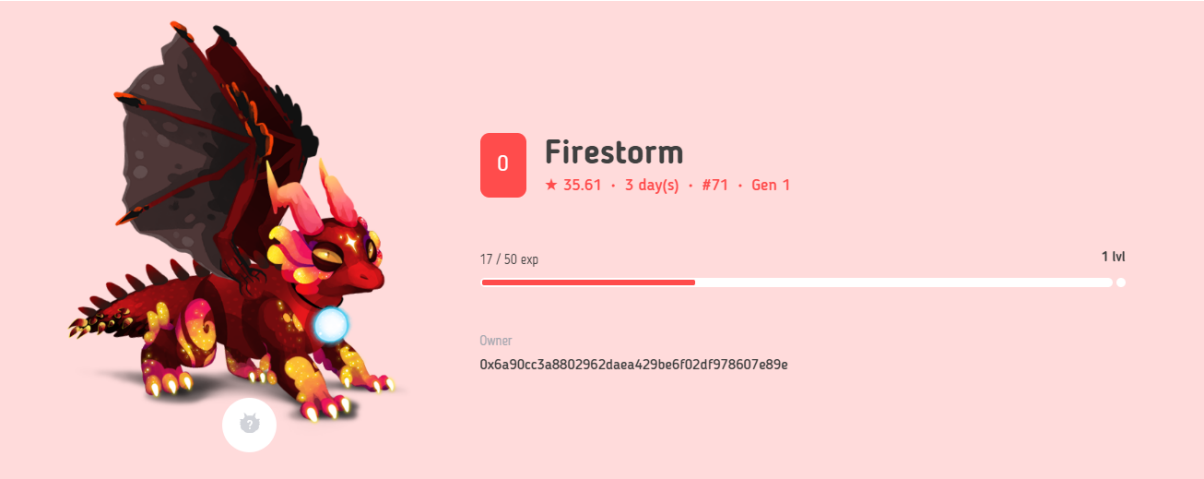

Figure 6: The dragon display, showing the image of the dragon, the dragon's name and the Dragon Skillfulness Indes on the left of the name.

The Dragon Skillfulness Index is calculated as follows:

$$I_{ds} = \sum_{k=1}^{40} P_g(k), \tag{4}$$

Where, I_{ds} is the Dragon Skillfulness Index, the gene points, P_g are calculated in Equation 5 below, and the index k runs from 1 to 40 for each gene in the dragon's genome as shown in Section 3.3 .

$$P_g = L_g * f_{gv} * f_{dr}, \tag{5}$$

Where L_g is the gene level, f_{gv} is the gene variety factor, and f_{dr} is the dominant or recessive factor, for a dominant gene $f_{dr} = 1$ and for a recessive gene $f_{dr} = 0.7$, described in Section 3.3. The gene variety factor for each dragon variety is given in Table 5.

4.1.6 Special attack and special defense skills

Special attack or *special defense* is the ability to use the special powers available to each dragon family. It improves the *attack* or *defense* during a battle move. Those special skills use Mana. In Table 6 the amount of Mana necessary for the activation of the *special*

Gene Variety	Codename	Gene variety factor
1 (inbreeding)	Inbreeding	0.5
2 (regular)	Common 0	1.2
3 (regular)	Common 1	1.2
4 (regular)	Common 2	1.2
5 (regular)	Common 3	1.2
6 (regular)	Rare 0	1.6
7 (regular)	Rare 1	1.6
8 (regular)	Rare 2	1.6
9 (mystery)	Epic 0	2.8
10 (mystery)	Epic 1	2.8

Table 5: The gene variation multiplier depending on the different dragon variations

attack or the *special defense* skill depending on the type of dragon is shown as well as the probability for its activation.

For dragons with a mixed genome as a result of the breeding process the type used for special skills is determined during the incubation process by a factored random and stored in the type field in the FightSkill structure (see Section 3.3).

Dragon type	Fire	Water	Earth	Air	Magic
	Special Attack skills details				
Mana points	$3 \times A$	$3 \times S$	$3 \times D$	$3 \times V$	$3 \times I$
Attack factor	$\sqrt{A/3} + 1$	$\sqrt{S/3} + 1$	$\sqrt{D/3} + 1$	$\sqrt{V/3} + 1$	$\sqrt{I/3} + 1$
Probability of activation	$\sqrt{I} + 10$	$\sqrt{I} + 10$	$\sqrt{I} + 10$	$\sqrt{I} + 10$	$\sqrt{I} + 10$
	Special Defense skills details				
Mana points	$3 \times A$	$3 \times S$	$3 \times D$	$3 \times V$	$3 \times I$
Attack factor	$\sqrt{A/3} + 1$	$\sqrt{S/3} + 1$	$\sqrt{D/3} + 1$	$\sqrt{V/3} + 1$	$\sqrt{I/3} + 1$
Probability of activation	$\sqrt{I} + 10$	$\sqrt{I} + 10$	$\sqrt{I} + 10$	$\sqrt{I} + 10$	$\sqrt{I} + 10$

Table 6: Table of Mana costs, multipliers for a attack/defense and a probability of activation for Special Attack and Special Defense.

4.1.7 Special peaceful skills

The maximum Level Up for a dragon is 10. On the 10th Level Up, the player can spend the DP acquired on *special peaceful skills* for their dragon.

A *special peaceful skill* allows users to earn in-game currency in exchange for offering skills to the game community on the game's marketplace[4].

A dragon can buy a *special peaceful skill* that can be used in order to receive a boost to one of its *basic skills as* shown in the first five rows of Table 7. After the boost has been applied, the *basic skill* defined in Equation 1 will become $Sk^{new}(j) = f_j \times Sk^{old}(j)$, with f_j being the Action Factor and j denoting the basic skill, $j \in$ A (attack), D (defense), S (stamina), V (speed), I (intelligence).This boost will be available to use for only one battle, thus incentivizing players to find an opponent and commence a battle as soon as they have bought the *special peaceful skill* and applied the boost to one of their *basic skills*. Alternatively, a player can buy a *special peaceful skill*, which will recharge the Health or Mana points of the dragon, bottom two rows of Table 7.

The dragon offering the *special peaceful skill* will have to use its Mana points to be able to offer the service. The amount of Mana points necessary for each different *special peaceful skill* is shown in column 2 of Table 7. The selling dragon will receive the in-game currency reward for the service it provided, and its Mana points will restore themselves over time.

Special peaceful skill	Action Factor	Mana points
Attack boost	$f_A = \sqrt{A/30} + 1$	$3 \times A$
Stamina boost	$f_S = \sqrt{S/30} + 1$	$3 \times S$
Defense boost	$f_D = \sqrt{D/30} + 1$	$3 \times D$
Speed boost	$f_V = \sqrt{V/30} + 1$	$3 \times S$
Intelligence boost	$f_I = \sqrt{I/30} + 1$	$3 \times I$
Healing	$H_R = 2 \times S$	$3 \times S$
Mana recharge	$M_R = 2 \times I$	$3 \times I$

Table 7: Table showing the different special skills that can be obtained (column 1), the Mana points the selling dragon needs to offer each skill (column 2) and the factor showing the increase in skill (column3).

4.2 Leveling up dragons and dragon population growth

Now that we explained how dragon skills are calculated we can talk about dragon population growth.

There is no hard cap on the number of dragons in the population. However, a dragon will be able to breed only if it has accumulated the required number of XP for a Dragon Level Up and as a result has acquired the necessary amount of DP.

At this point, a user will have to decide whether to upgrade their dragon (level up its body parts and get a stronger dragon) or to interbreed it with another dragon.

[4]The price of the *special peaceful skills*, alongside the prices of other items, such as dragons and eggs, traded on the marketplace will be decided by the market forces. The role of Dragonereum will only be to provide the internal marketplace to facilitate trade, however players will be able to interact directly with smart contracts and third-party marketplaces can be introduced.

Additionally, getting dragon offsprings will become more and more difficult when going up levels as the required amount of XP will increase from level to level. Therefore, it will be necessary to have, and to win more and more battles.

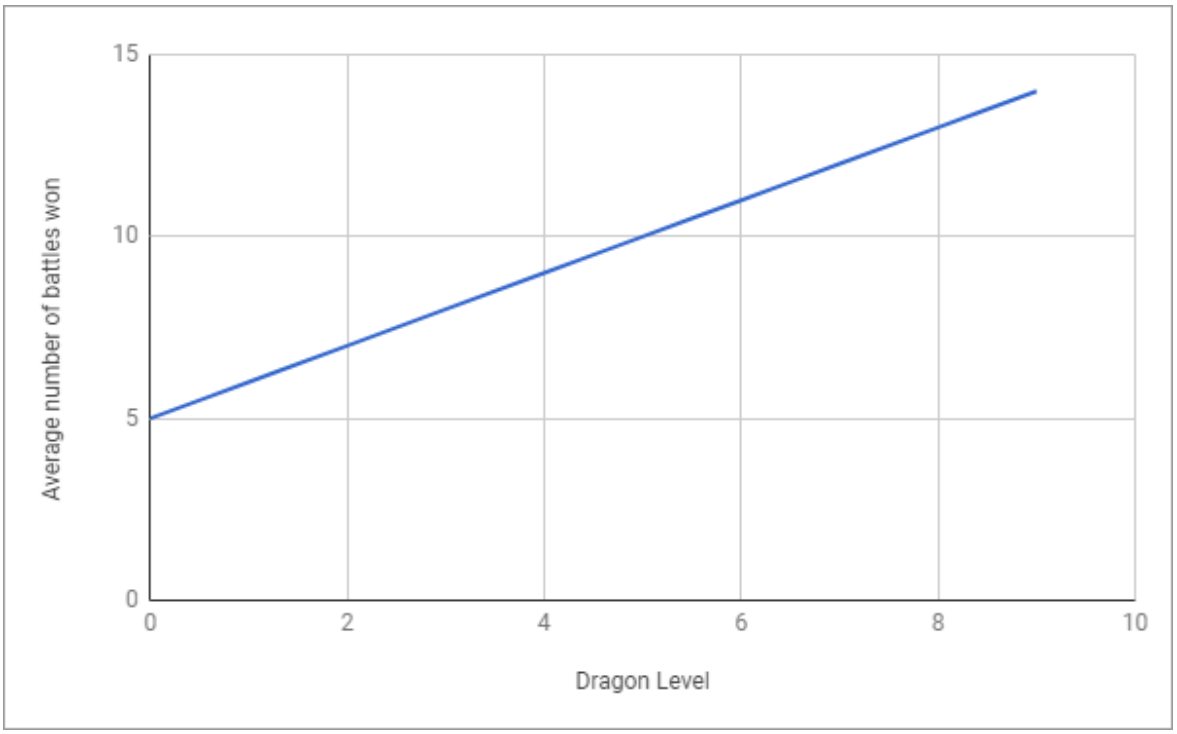

Figure 7: Average number of battles won required for a dragon Level Up

Before we describe the growing difficulty in acquiring DP we have to look at how the DS is calculated,

$$DS = 0.7 * A + 2.1 * D + 2.3 * S + 1.1 * V + 1.5 * I, \tag{6}$$

where A is the *attack*, D is the *defense*, S is the *stamina*, V is the *speed*, and I the *intelligence* of the dragon. The *basic skills* are calculated in Equation 1[5].

The constants in Equation 6 were carefully obtained through a rigorous simulation procedure ensuring that dragons with similar DS have an equal chance at winning the battle. Numerous battles between randomly chosen dragons with a similar amount of total basic skills were simulated and if there were battles where a dragon had an advantage, the values were adjusted in order to avoid this situation. The process was repeated until there were no dragons that had a winning advantage and every dragon, regardless of their skills or traits, has a 50% chance of winning against a dragon with a similar DS.

Based on the DS, the game's algorithms offer suitable opponents for training battles. A short description and the corresponding code for the training battles are given in the Appendix.

[5]In the equation $Sk(attack) \equiv A$, $Sk(defense) \equiv D$, $Sk(stamina) \equiv S$, $Sk(speed) \equiv V$, $Sk(intelligence) \equiv I$

As a result of these training battles the winners will receive XP. The number of XP won, in the case when the attacking dragon is the winner, is calculated according to the formulas below.

$$XP_e = \begin{cases} 10 * \left(\frac{DS_d}{DS_w}\right)^5 & \text{if } DS_d < DS_w \\ \left(\frac{DS_d}{DS_w}\right)^2 & \text{if } DS_d > DS_w, \end{cases} \tag{7}$$

where XP_e are the Experience Points earned after a battle, DS_d is the DS of the defeated dragon, and DS_w is the DS of the winning dragon. The factor of 10 in the case when $DS_d < DS_w$ is necessary in order to keep XP_e larger than one and in the same range as the points earned when $DS_d > DS_w$. In the case when the attacking dragon loses, and the defending dragon wins, it will receive $XP_e/2$. The reduction in the number of XP won is done in order to incentivize the attacking dragons, which use gas to initiate the transaction on Ethereum.

Once the required amount of XP is accumulated the dragon will get a dragon level up. There are ten Dragon Level Ups possible for each dragon. Each next dragon level up requires more XP and therefore more battles to be won, see Table 8.

At the same time the strongest dragon in the population will likely get less XP as a result of battles as it will become more and more difficult to find an opponent of the same or higher DS, thereby limiting the number of battles it can have on the one hand and minimizing the amount of XP it can obtain by winning battles on the other.

Dragon Level	Experience Points required for a level up
0	50
1	60
2	70
3	80
4	90
5	100
6	110
7	120
8	130
9	140
10	-

Table 8: The amount of XP required for a level up at each level (0-10).

Once a dragon goes up a level it receives DNA Points which are allocated according to Table 9 below.

Dragon Level	DNA Points received after leveling up
0	0
1	10
2	15
3	22
4	33
5	50
6	75
7	113
8	170
9	256
10	384

Table 9: The amount of DP received after leveling up at each level (0-10).

DP might be spent on:

- body parts level up
- breeding
- the acquisition of a *peaceful skill* (only after leveling up to the 10th dragon level).

Body part level ups will increase the total *basic skills* as is shown in Equation 1, since every body part level up gives a boost to the corresponding skills it is responsible for (see Table 1)[6]. The example of how this is calculated is given in Table 4 in Section 4.1.4.

The amount of DP required for a body part level up is calculated as follows:

$$C_{DP}(L_n) = Round(1.02 \times C_{DP}(L_{n-1})), \tag{8}$$

where $C_{DP}(L_n)$ is the cost of the body part level up at level L_n and $C_{DP}(L_{n-1})$ is the cost of the body part level up at level L_{n-1} correspondingly. The expression on the right hand side of the equation is rounded to the nearest hundredth, and this value is then used for the calculation of the cost at the next level and so on (the actual DP points are further rounded to the nearest integer). The first term in the series is $C_{DP}(L_0) = 10$, so 10 dP are required to level up a body part to level 1. The DP points required for leveling up a body part, calculated in Equation 8 are presented in Figure 8 as a function of the body part level.

[6]When the body part level up increases the active gene's level for that body part increases as well, since they are identical, however the levels of the other three genes in the body part set remain the same. From this arises the possibility that a dragon's offspring will inherit one of these three genes as its active gene and will have lower initial basic skills than its parents.

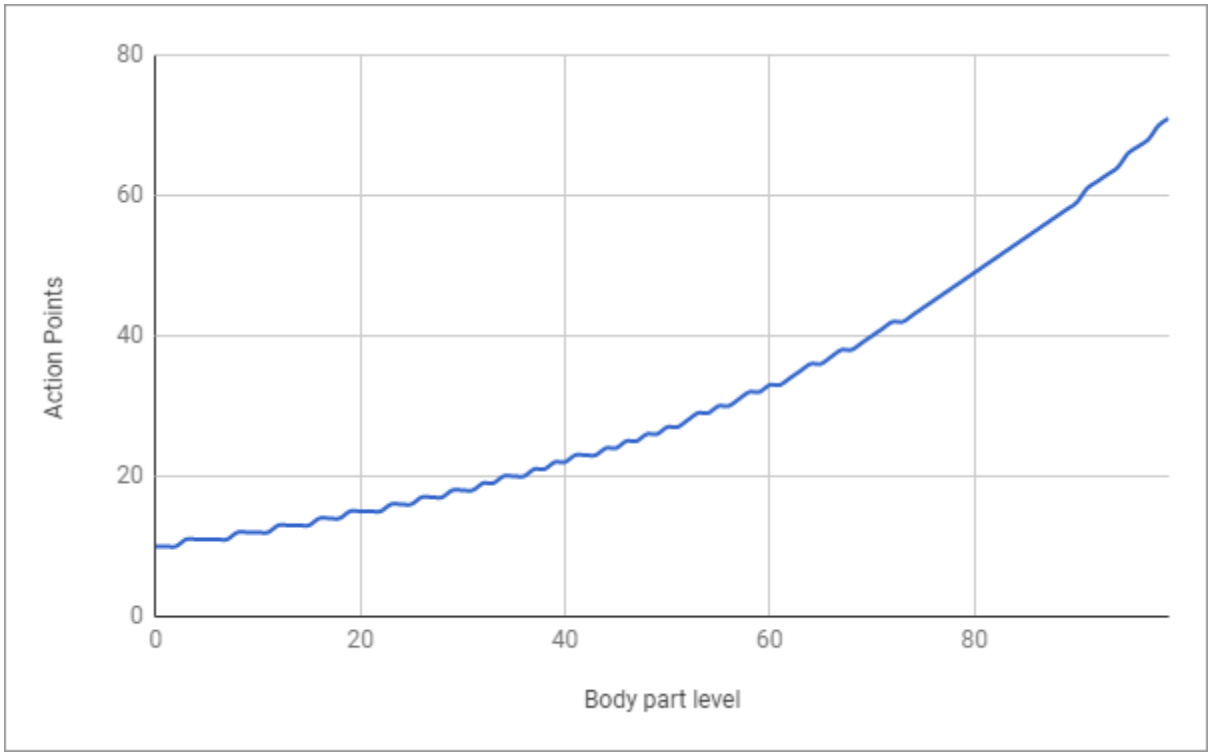

Figure 8: The amount of DNA Points necessary for a body part level up at each level (0-99)

Here we will look at the amount of DNA Points required for breeding at each level, see Table 10.

Dragon Level	DNA Points required for breeding
0	-
1	10
2	15
3	22
4	33
5	50
6	75
7	113
8	170
9	256
10	384

Table 10: The amount of DP required for breeding at each level (0-10).

As can be noted, the amount of DP received (see Table 9) and the amount of DP required for breeding (see Table 10) are the same at each level. Therefore, a dragon has a choice

between two options, it can either breed or upgrade its skills. The system will favor the spending of DP on breeding while on the same level where those DP were received, as once a dragon moves to the next level this amount of DP will only be sufficient for a body part level up.

Additionally, there is a game mechanism which prevents the situation in which dragons become very valuable regardless of their level and skills and every player decides to breed their dragon once it receives the first dragon level up from arising.

As a result of this mechanisms the overall dragon population will grow and the number of battles held will increase. Therefore, the amount of Gold distributed to battle winners will decrease making it more and more difficult to obtain the required amount for egg incubation.

On the other hand, dragons with higher DS will be able to receive Gold by being in the top of the leaderboards and by winning gladiator battles, thus creating incentive for other players to shift their playing style to produce higher valued dragons.

4.3 Early adopter advantage

As it was discussed in Section 2 the game has its own Gold account, where all unallocated Gold is held. It is used to reward battle winners and leaderboard entrants. The *battle winner reward* is calculated using Equation 9 below,

$$R = \left(\frac{G}{N_d^2}\right) * DS * 10 * f_{DS}, \tag{9}$$

*w*here R is the *battle winner reward*, G is the Gold balance in the game account, DS was defined in Equation 6 above, and f_{DS} is the *dragon strength factor* defined as,

$$DS_f = \begin{cases} \left(\frac{DS_d}{DS_w}\right)^8 & \text{if } DS_d < DS_w \\ \\ \frac{DS_d}{DS_w} & \text{if } DS_d > DS_w. \end{cases} \tag{10}$$

However, R, is subject to the following rules:

- If there are less than 15000 dragons in the population the maximum *battle winner reward* is 200 Gold coins
- If there is more than 15000 but less than 30000 dragons in the population, the maximum *battle winner reward* is 100 Gold coins
- Else (more than 30000 dragons) the *battle winner reward* is 25 Gold coins

Additionally, due to the early adopter advantage, it will be easier for those players that start participating in the game from its launch to earn Gold as well as to enter the leaderboard.

4.4 Case studies

The following simulations were conducted, using the initial parameters shown in Table 11[7].

ETH cost	200 USD
Gas price	5 Gwei
Egg incubation cost	1000 GOLD

Table 11: Initial parameters used in the case studies.

We study in detail three different cases. It should be noted that not all possible game features have been included in the simulations. For instance, a reward can be distributed to the top dragons on the leaderboard, and this was not incorporated as part of the cases studied below. De facto, these cases should be considered to be simplified situations, however they can be used as a very good gauge of the possible real life scenarios.

4.4.1 Case 1: Predominantly breeding (seldom leveling up)

Number of Battles	Population	Game account (GOLD)	Median battle reward (GOLD)	Median cost of Gold ($)	Cost of egg incubation ($)
500000	18300	30880000	35.37	0.025	25
1000000	26300	31840000	18.53	0.049	49
1500000	31600	32730000	13.24	0.068	68
2000000	35600	33170000	10.63	0.085	85
2500000	38800	33490000	9.06	0.099	99
3000000	41400	33630000	7.98	0.113	113

Table 12: Case Study 1: the number of battles held (column 1), the corresponding dragon population (column 2), the Gold in the game account (column 3), the median *battle winner reward* (column 4), the median cost of Gold in $ (column 5), and the cost of an egg incubation (column 6).

In this scenario players breed dragons with a 90% probability and level them up with a 10% probability. The game balance drops to around 30M GOLD and then settles at

[7]We are using values, which were typical for September of 2018.

approximately 33M GOLD as a result of the high volume of egg incubations, see Table 12 (column 3), and Figure 9 (black line). In Figure 9 the dragon population growth is shown as a function of the number of battles held. The number of battles in these case studies is a more appropriate variable than using a synthetic time, as it is problematic to predict the actual number of active players. The initial sharp growth of the dragon population is due to the distribution of genesis eggs.

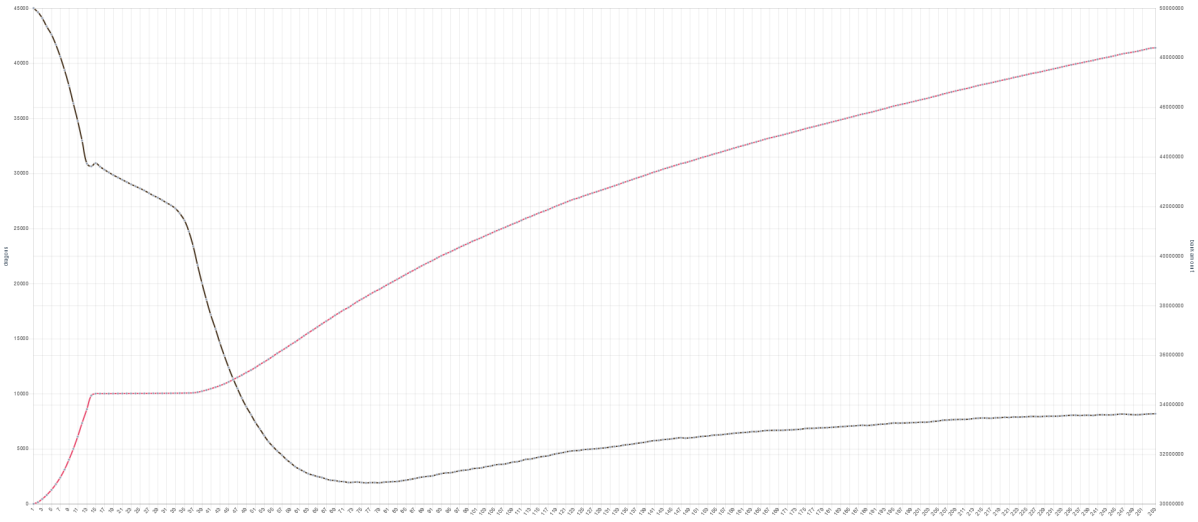

Figure 9: The number of dragons (red line), and the game account balance in GOLD (black line) as a function of the number of battles held.

The *battle winner reward* settles at 6.88 to 10.38 GOLD per battle depending on the DS. This small range of reward values can be explained by the fact that all dragons are of similar DS since the players do not level up dragons and spend all DP on breeding. The exact values of the median *battle winner reward* can be seen in Table 12 (column 4), and Figure 10 (dark blue line).

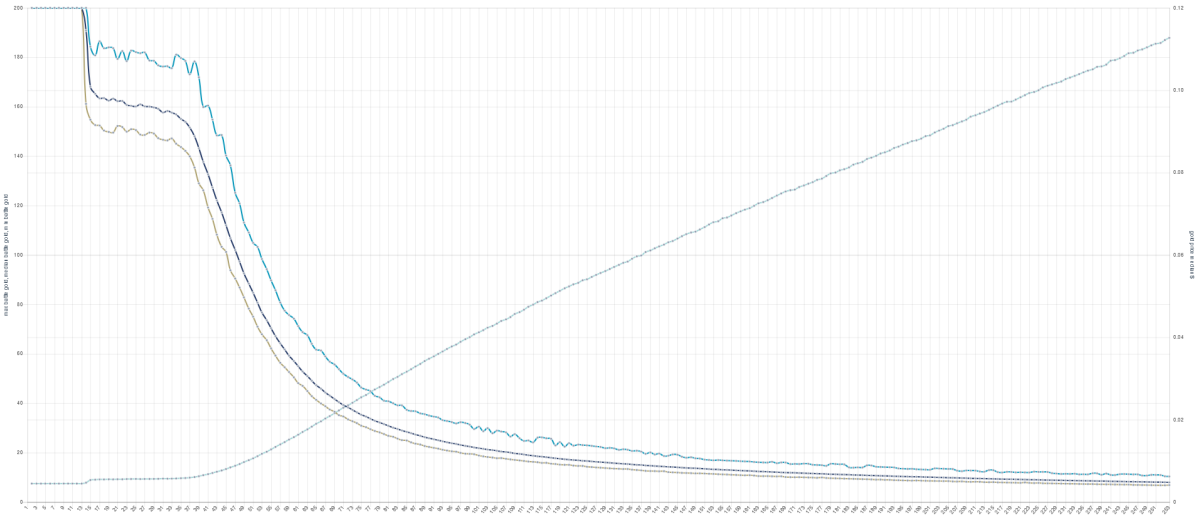

Figure 10: The cost of Gold in dollars calculated as a sum of mining fees cost (light blue line), and the median *battle winner reward* in Gold versus the number of battles held (dark blue line). The minimum (brown line) and the maximum (cyan) *battle winner reward* are also shown encasing the median *battle winner reward*.

In Figure 10 the cost of Gold in dollars calculated as a sum of mining fees cost necessary to mine the corresponding transactions is shown (light blue line) versus the number of battles held, which just like in Figure 9 is a variable that represents time in this synthetic environment. The cost of Gold grows because the amount of Gold distributed to winners reduces with the increasing number of battles held (see Section 4.3), making Gold more valuable.The median *battle winner reward* shown in the dark blue line decreases, as it depends on the amount of Gold in the game's account, see Equation 9, which also decreases as shown in Figure 9.

The mining cost for 1 GOLD is between \$0.086 and \$0.131, at 3,000,000 battles, Figure 10 (light blue line). It is calculated as: $\frac{C}{\bar{R}}$, where C is the cost of the transaction and $\bar{R}$ is the median *battle winner reward* (the median battle reward is shown as a function of the number of battles held in Figure 10).

The cost of an egg incubation in this case is between \$86 and \$131. This range comes from the fact that depending on who the winning dragons are there will be a different *battle winner reward* associated with them depending on their DS.

Therefore, economically motivated players will start leveling up dragons in order to get dragons of higher DS and earn more Gold in battles. As such, Case 1 is not in a stable state and will eventually turn into Case 2 portrayed below.

4.4.2 Case 2: Breeding and Leveling Up

Number of Battles	Population	Game account (GOLD)	Median battle reward (GOLD)	Median cost of Gold ($)	Cost of egg incubation ($)
500000	12200	18720000	55.54	0.016	16
1000000	15100	11400000	26.59	0.034	34
1500000	17800	8350000	16.51	0.055	55
2000000	20500	6950000	11.85	0.076	76
2500000	22900	6260000	9.5	0.095	95
3000000	25400	6110000	7.92	0.114	114

Table 13: Case Study 2: the number of battles held (column 1), the corresponding dragon population (column 2), the Gold in the game account (column 3), the median *battle winner reward* (column 4), the median cost of Gold in $ (column 5), and the cost of an egg incubation (column 6).

In this scenario players randomly breed and level up dragons. In our opinion this is the most likely scenario.

The game balance settles at approximately 6M GOLD. The *battle winner reward* settles between 3.64 and 26.15 GOLD per battle depending on the DS of the winning dragon.

In Figure 11, just as in Figure 9 the initial sharp growth of the dragon population is due to the distribution of genesis eggs (red line). The black line shows the amount of Gold in the game's account balance, which is declining due to the distribution of Gold to the battle winners. It will settle at approximately 6M GOLD once the number of battles held reaches 3,000,000, see also Table 13, column 3.

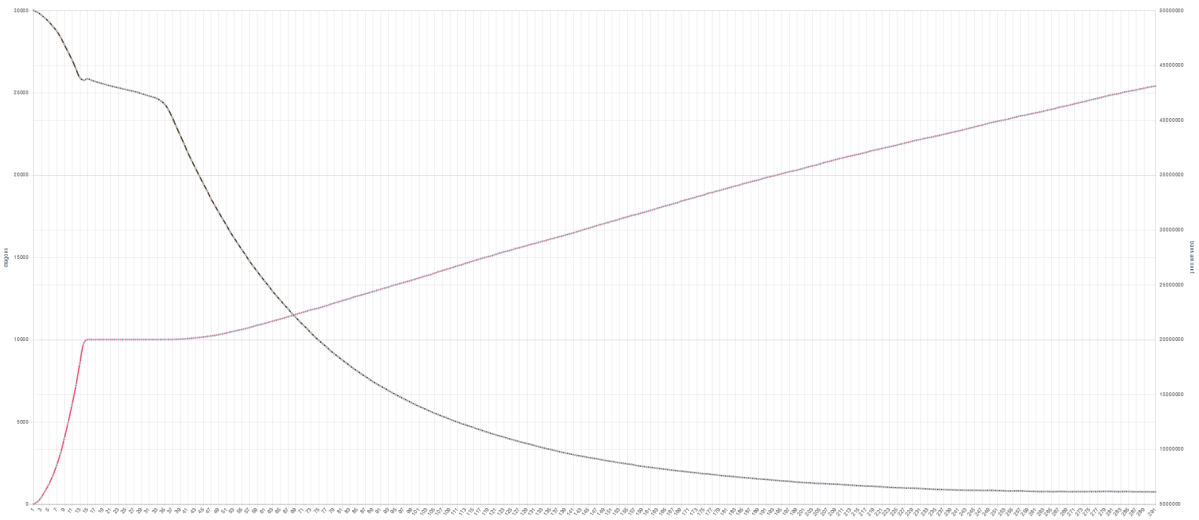

Figure 11: The number of dragons (red line), and the game account balance in Gold (black line) as a function of the number of battles held for Case Study 2.

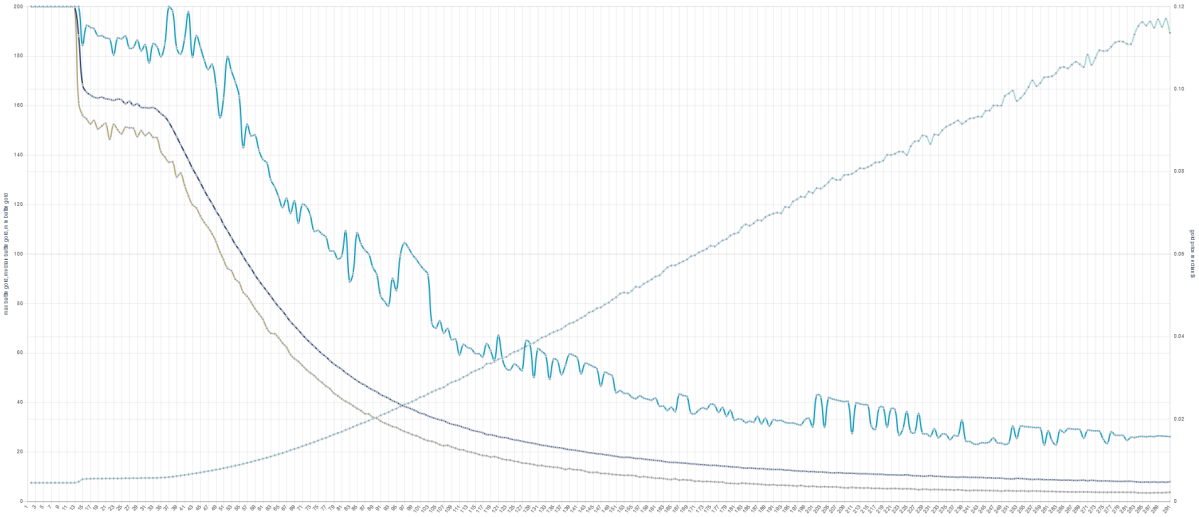

Figure 12: The cost of Gold in dollars calculated as a mining fee (light blue line), and the median *battle winner reward* in Gold versus the number of battles held (dark blue line) for Case Study 2. The minimum (brown line) and the maximum (cyan) *battle winner reward* are also shown encasing the median *battle winner reward*.

The mining cost for 1 GOLD is between \$0.034 and \$0.25, at 3,000,000 battles, see Table 13 (column 5), and Figure 12 (light blue line). The value of the mining cost will continue to grow with the increasing number of dragons and the *battle winner reward* will be reduced as was described in Section 4.3. The egg incubation cost in this case is between \$34 and \$250. This variation is due to the fact that each dragon has a corresponding DS, on which the *battle winner reward* depends (see Equation 9), so the *battle winner reward* will depend on which dragons are fighting at a given time, and the possible price of the egg incubation will have a spread depending on all the different possibilities. It should also be noted that in Figure 12, the maximum *battle winner reward* fluctuates due to the fact that it depends on the DS of the participating dragons. Therefore, if certain dragons with high DS are not participating in battles at some points this will affect the value of the maximum *battle winner reward*.

4.4.3 Case 3: Predominantly Leveling Up (seldom breeding)

Number of Battles	Population	Game account (GOLD)	Median battle reward (GOLD)	Median cost of Gold ($)	Cost of egg incubation ($)
500000	10000	14390000	66.83	0.013	13
1000000	10100	3176000	21.14	0.043	43
1500000	10800	543000	4.9	0.184	184
2000000	12100	101000	0.99	0.904	904
2500000	13200	0	0	Decided by the market	Decided by the market
3000000	Battles stop as no GOLD is distributed and dragons which reached the 10th level stop battling as they do not need additional experience				

Table 14: Case Study 3: the number of battles held (column 1), the corresponding dragon population (column 2), the Gold in the game account (column 3), the median *battle winner reward* (column 4), the median cost of Gold in $ (column 5), and the cost of an egg incubation (column 6).

In this scenario players level up dragons on all levels with a 90% probability and breed with a 10% probability.

The game balance drops to 0 GOLD at approximately 2,100,000 battles, as a result of the low amount of fees collected for egg incubations, as is seen in Figure 13, and in column 3 of Table 14. Therefore the *battle winner reward* will not be paid. This is shown in Figure 14, where the *battle winner reward* drops sharply to zero with the number of battles held (dark blue line). Just before that at 2 million battles the median *battle winner reward* will be 0.99 GOLD, and the median mining cost of Gold will be $0.904. After that once the game balance is at 0 GOLD, the price cannot be predicted. The price of Gold cannot be estimated due to the fact that when there is no Gold in the game account, the model assumes that the price of Gold is equal to the transaction fees price divided by zero (or another very small amount), thus making it too big to display on the graph.

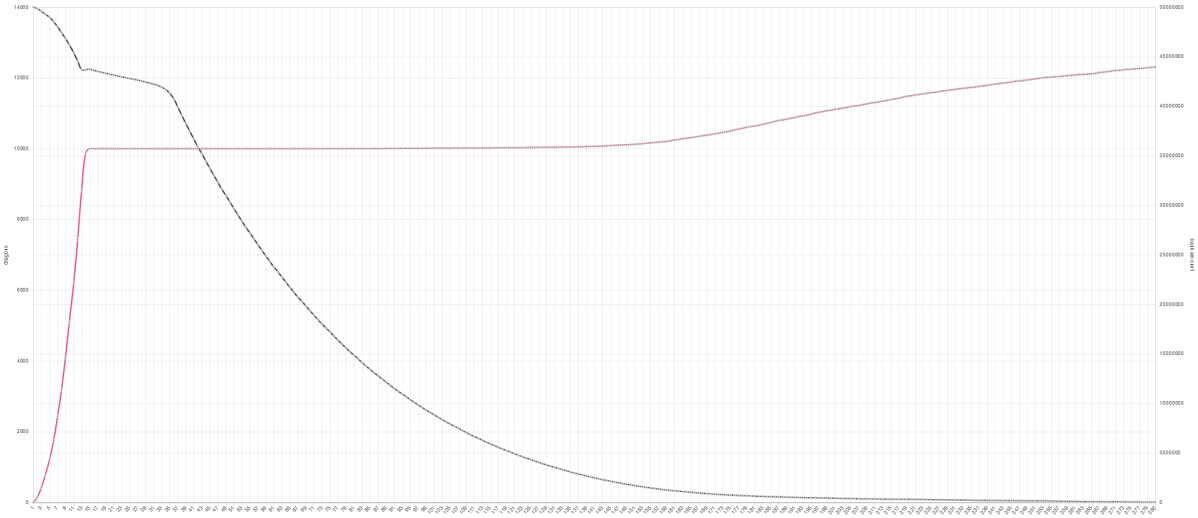

Figure 13: The number of dragons (red line), and the game account balance in Gold (black line) as a function of the number of battles held for Case Study 3.

Gold can be obtained from other players and therefore its price can not be determined by this simulation. The egg incubation cost also goes up and becomes unfeasible for the majority of players.

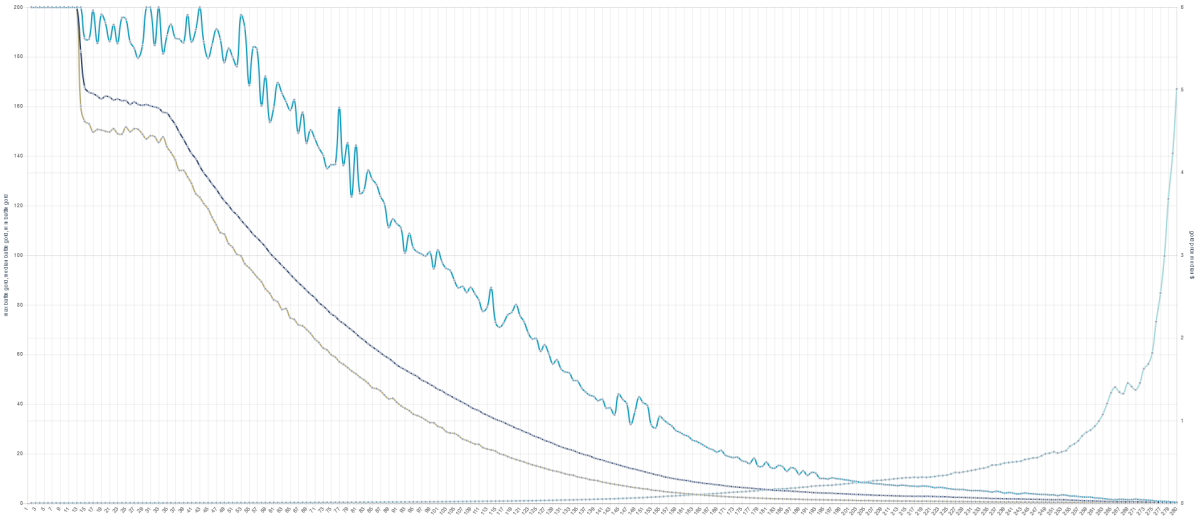

Figure 14: The cost of Gold in dollars calculated as a mining fee (light blue line), and the median *battle winner reward* in Gold versus the number of battles held (dark blue line) for Case Study 3. The minimum (brown line) and the maximum (cyan) *battle winner reward* are also shown encasing the median *battle winner reward*.

Therefore, the game slows down and no new dragons are created. However, this is not critical as the initial *battle winner reward* is not a goal of the game but just a mechanism to start up the in-game economy. Our aim is the creation of the game ecosystem where

users will offer different goods and services to each other and those goods and services will be exchanged for Gold (healing, buffs) or acquired with the help of Gold (bets on dragon battles).

Additionally, as the price of dragons will become higher more players will switch to breeding dragons therefore bringing the game to the state portrayed in Case 2.

These synthetic tests confirm that the aim to create a game ecosystem which is stable in the long term was achieved. The explored scenarios might not include all the possible options for the players' behaviour, nonetheless, they offer an insight on how the game ecosystem might develop after the launch. It is shown that due to the system of feedback loops implemented in the game, that all three cases are going to end up in the equilibrium state of Case Study 2.

5 Implementation Details

5.1 Serverless application

Modern centralized games heavily rely on the entities that have created those games and that have full control over every aspect of the game: what to consider as a "bad" or "good" behaviour, private data policies, controls over the servers and all the data stored there, and determining the overall direction of the game development [7], [8], [9][8], [10], [11].

At the same time a number of technologies unrelated to the gaming industry has been emerging which let users enjoy a transparent, censorship resistant, trustless, programmable and permissionless environment where anyone has full control over their private data (this technology stack is often referred to as Web 3.0 [12], [13].

We think that It would be great to create a full scale game built on top of those technologies, so the created game will be 100% autonomous and decentralized, and no party will have control over any element of the game or its delivery mechanisms once it is launched, while still remaining engaging and fun compared to its centralized siblings.

However, with Dragonereum our aim is more realistic and it is to create a decentralized game built on the Ethereum network which will have minimal ties to our servers at launch and gradually move to decentralized solutions (storage, naming services and indexing) once the game is released.

In the long run and with the advancement of technology, we hope to remove any user dependency on us or on any other third party and switch to a fully autonomous and decentralized mode.

The game is currently accessible via browser with a MetaMask plugin installed (https://metamask.io/).

No sign up or any kind of registration is required as in order to offer engaging gameplay no one needs to know the names or any other personal information of the players. The private keys which are stored in the MetaMask wallet are sufficient to serve as the players' IDs.

The data layer consists of two ERC721 [14] non-fungible tokens which will represent two states of a dragon (an egg and a dragon) and an ERC20 [15] which will represent the in-game cryptocurrency.

The business logic layer consists of several smart contracts: egg core features contract, dragon core features contract, breeding, battling, marketplace and auth contract.

The game itself can be used without reliance on a back-end server for any purposes other than allowing users to derive the app from the server to the player's browser. The app uses client-side rendering, therefore, our server is actually just a storage which can be easily replaced.

[8]Sort the table by organization type (3rd column) and see the gaming entries.

However, to make the life of players a bit easier another back-end server is used for:

- Filtering of items offered on marketplaces
- Storage and delivery of notifications while a player is not online.

While the filtering server stores complete information about every item offered on the game's marketplaces, the client side application only receives the list of items in a required order. This feature can easily be turned off in the app settings so the app can be used without it.

Full scale decentralization is our long term goal and once the game has all the core functionality we will add new solutions and services from a Web 3.0 stack.

5.2 Off-chain solutions (state chains)

In Section 3.1 we discussed the current limitations associated with decentralized technologies and explained the steps taken in building Dragonereum with these limitations in mind. Another possible way of resolving the effects of the transaction costs, the associated delays with transaction processing and network congestion issues on the Ethereum network is with the use of off-chain (state-chain) solutions. In the following we describe a few of the most promising off-chain approaches for resolving the scalability issue.

The transaction cost in the Ethereum network is quite high, especially in the context of decentralized games with a rich game environment. We expect that our players will breed dragons, attack opponents and participate in battles tens or hundreds of times per day. On average every action will cost a million of gas points. Even with minimal gas price, gaming costs will be sufficient and might scare away some players.

Additionally, as it was discussed in Section 3.1, another issue with Ethereum is that the transaction processing (confirmation) time is several orders of magnitude higher than players are used to nowadays in multiplayer games. This obstacle significantly decreases the players' experience in decentralized games and therefore a much more engaging game can be created if this obstacle is removed.

The third factor we need to consider, when developing a decentralized game, is the network availability. Every decentralized app is technically "unstoppable" in virtue of its decentralized nature and it will be working for the user as long as the user has a connection to the Ethereum network. However, in practice dapps don't have 100% availability: network congestion during initial coin offerings, network attacks[9] or the release of some popular dapp can lead to an enormous surge in the gas price. This surge leads to the situation when the transaction's gas costs more than the value, which the user can receive from the usage of the dapp. Despite the fact that dapps stay technically available (the

[9]The situation where a malicious entity attacks the Ethereum blockchain by sending a large amount of transactions with a high gas price in order to suppress the transactions of regular users from being mined.

user can put an extremely high gas price and the transaction will be included in the next block), they become "financially unavailable" for most of their users.

5.2.1 State channels

State channels are a technique for performing transactions and other state updates "off chain". However, things that happen "inside" of a state channel still retain a very high degree of security and finality: if anything goes wrong, there is still the option of referring back to the on-chain dispute. This allows the users to perform transactions with much lower transaction fees and with lower confirmation times.

However, state channels are useful only if the participants are going to be exchanging many state updates over a long period of time, and the set of participants must be defined in advance.

5.2.2 Sharding

In the sharding approach, the blockchain is split into different sections called shards, each of which can independently process transactions. Blocks in shards are called collations. Consensus on shards depends on main chain, which is connected with shards by a special contract on the main chain called Validator Manager Contract (VMC). The VMC is responsible for a Proof-of-stake system, collation header validation and cross-shard communication. With this approach, transactions in separate shards can be processed in parallel, and this could significantly increase the scalability of such a system.

To the best of our knowledge, currently, there is no public blockchain with an integrated sharding mechanism, which is suitable for usage.

5.2.3 Plasma

Plasma is a novel technique that could enable Ethereum to reach many more transactions per second than are currently possible [16]. Like state channels, Plasma is a technique for conducting off-chain transactions while relying on the underlying Ethereum blockchain to ground its security.

But Plasma takes the idea in a new direction, by allowing for the creation of "child" blockchains attached to the "main" Ethereum blockchain. These child-chains can, in turn, spawn their own child-chains, which can spawn their own child-chains, and so on. The result is that many complex operations can be performed at the child-chain level, running entire applications with many thousands of users, with only minimal interaction with the Ethereum main-chain. A Plasma child-chain can move faster, and charge lower transaction fees, because operations on it do not need to be replicated across the entire Ethereum blockchain.

However this concept is under development right now, and there is no open and mature implementations as of the date of writing.

5.2.4 TrueBit

Truebit is a technology to help Ethereum conduct heavy or complex computations off-chain (https://truebit.io). This makes it different from state channels and Plasma, which are more useful for increasing the total transaction throughput of the Ethereum blockchain.

The TrueBit design allows for compact proofs to be created off-chain to submit to the Ethereum blockchain, which is necessary to Dragonereum for breeding and battle use cases.

However, those computations are carried out and verified by Truebit participants for a fee, thus adding additional costs to the process, which makes this solution less attractive for our use-cases.

5.2.5 zk-SNARKS off-chain validation(ZoKrates)

Non-interactive proofs of computation allow for one to have significant benefits in scalable computation [17]. With zk-SNARKs/STARKs we can perform the breeding and battle calculation off-chain and submit the result together with the zk-SNARK proof to the Ethereum blockchain.

However, the drawback of this approach is the high gas usage, which is higher or similar to our algorithms deployed directly to a smart contract. Also, there is a scalability issue, as only around six such computations can be stored in a single block. Additionally, as stated by the developers: "this is a proof-of-concept implementation. It has not been tested for production" [17].

If the validation gas cost will be reduced in the future, we can take this approach under consideration again.

5.2.6 Sidechains

The term "sidechains" was first described in [18]. It is a mechanism where by proving that a user had "locked" some coins/tokens that were previously in their possession, they were allowed to move some other coins/tokens within a sidechain.

A sidechain can be used to offload computations from another chain. Individual sidechains can have different consensus logic from the mainchain, which means they can be optimized for applications that require extremely high speeds or heavy computation, while still relying on the mainchain for issues requiring the highest levels of security.

However, sidechains can increase scale but do not imply scalability. Sidechains are no better at providing scalability than increasing the block size. What sidechains bring is the ability to build networks that run on different – and possibly better-scaling – technology.

The main advantage of sidechains solutions is that it is already working today and can be integrated into Dragonereum's system.

After carefully investigating the available off-chain solutions, we have concluded that at present they do not offer a viable solution for our game design, as they are not production ready yet. We shall keep the possibility for a future integration open. However, at this stage our game design was built with the current limitations of the Ethereum's blockchain bandwidth in mind, and there is no real necessity to go off-chain. Furthermore, by staying on-chain we have the advantage of remaining more secure, while the above third-party solutions might have certain vulnerabilities associated with them, especially if they have not been released and tested out yet. Another benefit from not relying on third parties is the fact that our system will not become dependent on solutions that might be suspended or abandoned at any point in time.

5.3 Graphics

While designing the game we considered several options for visualisation style of our dragons. urrent status quo in cryptocollectible industry is use of flat, simplified images which are easily merged into an image of a game character.

However, we decided to switch to 3/4 view as it gives more realistic perspective to players and it makes the potential transition to VR or AR a bit easier.

6 Possible Integrations

6.1 Prediction markets

There are many game events which can be used as a base for a prediction, for example, battle winners and leaderboard entrants. Since in Dragonereum everything is kept on-chain, third-party services such as Augur (https://www.augur.net/) can be used to place bets on events and outcomes stored in the game's smart contracts (even those that we can not predict at the moment).

With the current implementation of the Augur ecosystem we do not see the possibility to bet on small events (such as the outcome of a training battle), however, other betting services (DiceyBit https://diceybit.com) already offer those capabilities with the use of data supplied by the game developers through an API. On the other hand, Augur can be used for larger scale events, such as predicting the maximum Dragon Skillfulness Index at a future date.

6.2 Trading protocols

In addition to the in-house marketplaces for game tokens such as dragon eggs (ERC721), dragons (ERC721) and Gold (ERC20) the decentralized nature of the tokens will allow them to be traded on other global trading platforms.

We prefer this to happen in an open and decentralized manner as all the information about each token is publicly accessible and there is no need to rely on any third party. Therefore, the best option for this is the decentralized liquidity networks and exchanges.

Joining the decentralized liquidity network Bancor will provide instant liquidity for Gold and enable its convertibility to other connected tokens and vice versa with low fees and no trading spread.

Additionally, all game tokens are compliant with the 0x's protocol V2 therefore all of them can be traded on 0x relayers when V2 of 0x's protocol will be launched.

The compliance of Dragonereum's ERC721 tokens with the Wyvern Protocol (https://www.projectwyvern.com/) will enable gas-free and escrow-free auctions (sell orders) on platforms such as Opensea.io.

6.3 Virtual worlds

Bringing Dragonereum's dragons into the virtual reality of Decentraland (https://decentraland.org) will make the gaming experience even more engaging and immersive.

For example, players will be able to witness dragon battles and find hidden dragon eggs.

Additionally, connecting Dragonereum's marketplaces to Decentraland's economy and community will allow for a higher engagement on the game's marketplaces.

At the first stage Dragonereum will have its own world in Decentraland (land in Genesis City) which will serve as a basis for future VR capabilities and features.

6.4 Messenger integrations

Easy access to the Ethereum blockchain will make the world a more open and transparent place. Therefore we advocate the use of the game in messenger platforms which will allow interaction with the game through text based contracts, interfaces and bots. We looked at the early releases of the Status messenger and our smart-contracts are fully compatible with it.

6.5 Location based protocols

Use of location based protocols will bring new dimensions into the Dragonereum's gameplay. The thought core game design will much likely stay unchanged, however we will create new location based game mechanics in order to utilize the power of proof-of-location protocols such as control by a dragon or a thunder of dragons over countries or territories.

7 Genesis

An initial distribution of genesis eggs will be conducted during the game's launch. 10 000 genesis eggs will be distributed in total (2000 of each egg type). Types of eggs (water, fire, air, earth, and magic) will be distributed on a sequential basis. Genesis eggs store pure types of dragons without additions from other types.

Each new genesis egg will be available for a claim once per block.

The eggs will be free to claim, however the amount of gas used by genesis transactions will be artificially increased in order to make genesis eggs and dragons more valuable.

Excessive gas will be used to write down Dragonereum's story to the Ethereum blockchain.

As Gold is required for egg incubation, genesis eggs will be distributed together with the required amount of Gold. Genesis eggs do not store any information about parents, therefore, a player will not be able to predict the value and rarity of a dragon which will be hatched from a particular genesis egg.

The distribution of body parts during genesis is shown in Table 15.

Body part	Percentage
inbreeding	0
common 0	0.30
common 1	0.24
common 2	0.22
common 3	0.19
rare 0	0.025
rare 1	0.015
rare 2	0.01
epic 0	0
epic 1	0

Table 15: The percentage distribution of the different body parts according to their variety.

8 Token Distribution

There will be 60,000,000 GOLD minted during product deployment and no new coins will be added. Gold will be allocated as shown in Figure 15.

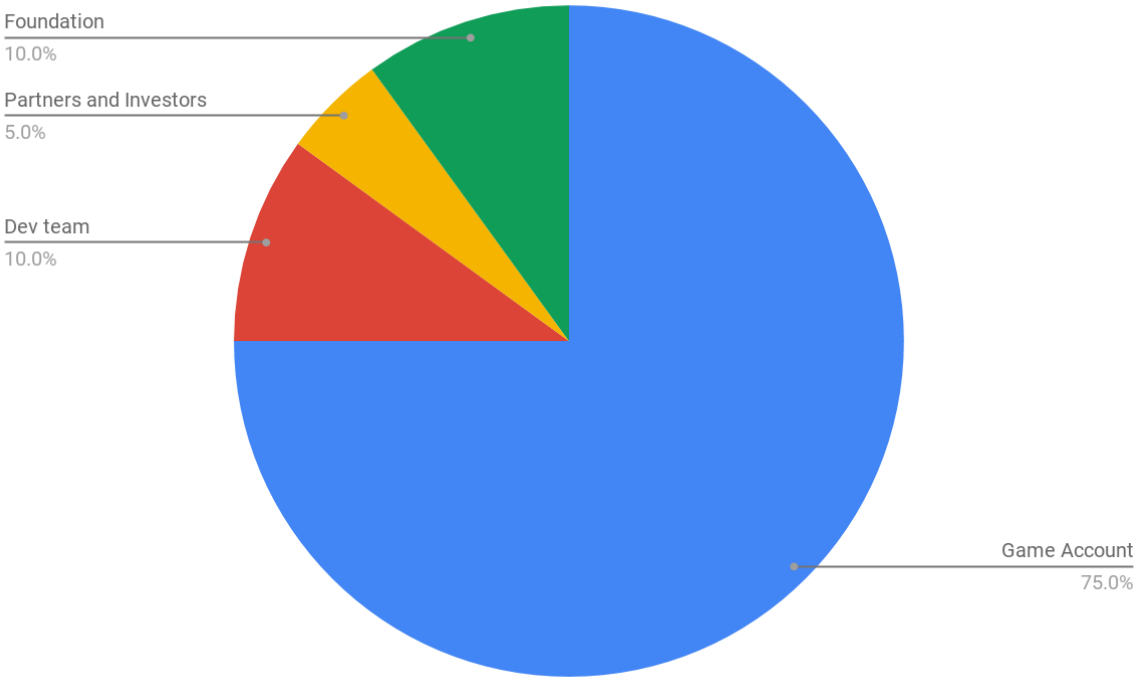

Figure 15: Chart showing the allocation of Gold.

Game account

As Dragonereum will not have any kind of initial coin offerings or a sale, the majority (75%) of tokens will be allocated to the game account (shown in blue in Figure 15).

Development team and partners

Once the smart contract is deployed appointed team members will receive a total of 10% of tokens in their possession (shown in red in Figure 15).

Another 5% will be booked for the future partners and investors (shown in yellow in Figure 15).

Foundation

The remaining 10% will be used for the Dragonereum ecosystem development and community building (shown in green in Figure 15). This may include (but not necessarily):

- New team members and advisors
- Liquidity pool (eg. Bancor)

- Airdrop
- Security audits
- Bounty campaigns (eg. Gitcoin).

9 Conclusion

In this document we described a blockchain cryptocollectible PvP game built on the Ethereum network which emphasizes the advantages of the blockchain solutions for future blockchain gaming, gambling and collectible markets.

The technological and socioeconomic solutions for creation of a sustainable game ecosystem were examined and discussed.

A thorough description of the game's details and rules was provided. Further, we showed that Dragonereum is made with the current constraints of the blockchain technology in mind.

A description of the in-game cryptocurrency, Gold, was given and it was shown that its value will grow.

In addition, we presented a large variety of possible future integrations of the game.

Please join our official Telegram channel for regular news and updates:

https://t.me/dragonereum

References

[1] Tomas Draksas. *Dev. Update #6: Edgeless Dice RNG*. 2017, Aug 28. URL: https://medium.com/edgeless/dev-update-6-edgeless-dice-rng-daef755f26a0.

[2] Oraclize. *random-datasource*. 2017, May 18. URL: https://github.com/oraclize/ethereum-examples/tree/master/solidity/random-datasource.

[3] Ksenya Serova Dao Casino. *Dao Casimo White Paper*. 2017, Jun 27. URL: https://github.com/DaoCasino/Whitepaper/blob/master/DAO.Casino%20WP.md.

[4] Gluk256. *The Signidice Algorithm*. Accessed: 2016, Aug 26. URL: https://github.com/gluk256/misc/blob/master/rng4ethereum/signidice.md.

[5] SECBIT. *How the winner got Fomo3D prize – A Detailed Explanation*. 2018, Aug 22. URL: https://medium.com/coinmonks/how-the-winner-got-fomo3d-prize-a-detailed-explanation-b30a69b7813f.

[6] Dragonereum. *How to breed Dragons on the blockchain*. 2018, March 26. URL: https://medium.com/@dragonereum/how-to-breed-dragons-on-the-blockchain-e7b4c8cad2c0.

[7] Gogo. *PLAYERUNKNOWN'S BATTLEGROUNDS*. 2018, Jun 16. URL: https://steamcommunity.com/app/578080/discussions/1/2788173147744268307/.

[8] Steam. *Banned by Game Developer (Game Ban)*. 2017. URL: https://support.steampowered.com/kb_article.php?ref=6899-IOSK-9514.

[9] WikipediA. *List of data breaches*. 2018. URL: https://en.wikipedia.org/wiki/List_of_data_breaches.

[10] Ben Gilbert. *Major changes are coming to 'Fortnite' and the most popular player in the world isn't happy about it*. 2018, Jun 22. URL: https://www.businessinsider.com/fortnite-changes-building-resource-ninja-2018-6.

[11] Aaron Mamiit. *Blizzard Secretly Made 'World Of Warcraft' Enemies More Powerful, And Players Are Not Happy About It*. 2017, Mar 30. URL: https://www.techtimes.com/articles/203499/20170330/blizzard-secretly-made-world-of-warcraft-enemies-more-powerful-and-players-are-not-happy-about-it.htm.

[12] Josh Stark. *Making Sense of Web 3*. 2018, Jun 6. URL: https://medium.com/l4-media/making-sense-of-web-3-c1a9e74dcae.

[13] Stephan Tual. *Web 3.0 Revisited - Part One: "Across Chains and Across Protocols"*. 2017, May 26. URL: https://blog.stephantual.com/web-3-0-revisited-part-one-across-chains-and-across-protocols-4282b01054c5.

[14] Ethereum. *ERC: Non-fungible Token Standard #721*. 2017, Sep 26. URL: https://github.com/ethereum/eips/issues/721.

[15] Ethereum. *ERC: Token standard #20*. 2015, Nov 19. URL: https://github.com/ethereum/eips/issues/20.

[16] Josh Stark. *Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit*. 2018, February 12. URL: https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4.

[17] Jacob Eberhardt. *ZoKrates*. 2018. URL: https://github.com/JacobEberhardt/ZoKrates.

[18] Adam Back et al. *Enabling Blockchain Innovations with Pegged Sidechains*. 2014, Oct 22. URL: https://blockstream.com/sidechains.pdf.

Appendix

Training Battles

Below is the code describing the execution of the training battles.

```
   function _resetBlocking(Dragon dragon) internal pure returns (Dragon) {
        dragon.blocking = false;
        dragon.specialBlocking = false;
        return dragon;
    }

    function _attack(uint8 turnId, bool isMelee, Dragon attacker, Dragon opponent, uint8
_random) internal pure returns (Dragon, Dragon) {
        uint8 _turnModificator = 10; // multiplied by 10
        if (turnId > 30) {
            // _turnModificator = uint8(1 * 10 + uint16((turnId - 30) * 10 * 5) / 40);
            // hack "stack too deep" error
            uint256 _modif = uint256(turnId).sub(30);
            _modif = _modif.mul(50);
            _modif = _modif.div(40);
            _modif = _modif.add(10);
            _turnModificator = _modif.toUint8();
        }

        bool isSpecial = _random < _multiplyByFloatNumber(attacker.specialAttackChance,
_turnModificator);
        uint32 damage = _multiplyByFloatNumber(attacker.attack, _turnModificator);
        if (isSpecial && attacker.mana >= attacker.specialAttackCost) {
            attacker.mana = attacker.mana.sub(attacker.specialAttackCost);
            damage = _multiplyByFloatNumber(damage, attacker.specialAttackFactor);
        }
        if (!isMelee) {
            damage = _multiplyByFloatNumber(damage, DISTANCE_ATTACK_WEAK__);
        }
        uint32 defence = opponent.defence;
        if (opponent.blocking) {
            defence = _multiplyByFloatNumber(defence, DEFENCE_SUCCESS_MULTIPLY__);
            if (opponent.specialBlocking) {
                defence = _multiplyByFloatNumber(defence, opponent.specialDefenceFactor);
            }
        } else {
            defence = _multiplyByFloatNumber(defence, DEFENCE_FAIL_MULTIPLY__);
        }
        if (damage > defence) {
            opponent.health = _safeSub(opponent.health, damage.sub(defence));
        } else if (isMelee) {
            attacker.health = _safeSub(attacker.health, defence.sub(damage));
        }

        return (attacker, opponent);
    }

    function _defence(Dragon attacker, uint256 initialSeed, uint256 currentSeed) internal
pure returns (Dragon, uint256) {
        uint8 specialRandom;
```

```
        (specialRandom, currentSeed) = _getRandomNumber(initialSeed, currentSeed);
        bool isSpecial = specialRandom < attacker.specialDefenceChance;
        if (isSpecial && attacker.mana >= attacker.specialDefenceCost) {
            attacker.mana = attacker.mana.sub(attacker.specialDefenceCost);
            attacker.specialBlocking = true;
        }
        attacker.blocking = true;
        return (attacker, currentSeed);
    }

    /* solium-disable-next-line security/no-assign-params */
    function _turn(
        uint8 turnId,
        uint256 initialSeed,
        uint256 currentSeed,
        uint32 distance,
        Dragon currentDragon,
        Dragon currentEnemy
    ) internal view returns (
        Dragon winner,
        Dragon looser
    ) {
        uint8 rand;

        (rand, currentSeed) = _getRandomNumber(initialSeed, currentSeed);
        bool isAttack = rand < currentDragon.attackChance;

        if (isAttack) {
            (rand, currentSeed) = _getRandomNumber(initialSeed, currentSeed);
            bool isMelee = rand < currentDragon.meleeChance;

            if (isMelee && distance > MAX_MELEE_ATTACK_DISTANCE) {
                distance = _safeSub(distance, currentDragon.speed);
            } else if (!isMelee && distance < MIN_ATTACK_DISTANCE) {
                distance = _min(MAX_DISTANCE, _multiplyByFloatNumber(currentDragon.speed,
FALLBACK_SPEED_FACTOR__));
            } else {
                (rand, currentSeed) = _getRandomNumber(initialSeed, currentSeed);
                (currentDragon, currentEnemy) = _attack(turnId, isMelee, currentDragon,
currentEnemy, rand);
            }
        } else {
            (currentDragon, currentSeed) = _defence(currentDragon, initialSeed, currentSeed);
        }

        currentEnemy = _resetBlocking(currentEnemy);
        if (currentDragon.health == 0) {
            return (currentEnemy, currentDragon);
        } else if (currentEnemy.health == 0) {
            return (currentDragon, currentEnemy);
        } else if (turnId < MAX_TURNS) {
            return _turn(turnId.add(1), initialSeed, currentSeed, distance, currentEnemy,
currentDragon);
        } else {
            uint32 _dragonMaxHealth;
            uint32 _enemyMaxHealth;
            (_dragonMaxHealth, ) = getter.getDragonMaxHealthAndMana(currentDragon.id);
            (_enemyMaxHealth, ) = getter.getDragonMaxHealthAndMana(currentEnemy.id);
```

```
            if (_calcPercentage(currentDragon.health, _dragonMaxHealth) >=
_calcPercentage(currentEnemy.health, _enemyMaxHealth)) {
                return (currentDragon, currentEnemy);
            } else {
                return (currentEnemy, currentDragon);
            }
        }
    }
```