2022 IEEE 7th International conference for Convergence in Technology (I2CT)
Pune, India. Apr 07-09, 2022

Gene Determination Algorithm: A Blockchain-based Case Study of Crypto Kitties

Tanu Gupta
Dept. of Computer Science & Engg.
Indian Institute of Technology (ISM)
Dhanbad, India 826004
tanugupta3.20mt0425@cse.iitism.ac.in

Dharavath Ramesh
Dept. of Computer Science & Engg.
Indian Institute of Technology (ISM)
Dhanbad, India 826004
drramesh@iitism.ac.in

Rahul Mishra
Dept. of Computer Science & Engg.
Indian Institute of Technology (ISM)
Dhanbad, India 826004
rahul.18dr0107@cse.iitism.ac.in

2022 IEEE 7th International conference for Convergence in Technology (I2CT) | 978-1-6654-2168-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/I2CT54291.2022.9825042

***Abstract*—Crypto Kitties is one of the most well-known games built on the Ethereum blockchain and has been in operation for a longer time. This paper examines the market's fairness by focusing on the gene determination algorithm required for breeding two kittens. This method has very little unpredictability, and as a result, players who understand it have a considerable edge over those who do not. Furthermore, this paper demonstrates a methodology that aims to increase randomness in the gene determination algorithm by associating it with a discrete crossover operator. In the end, this paper addresses some of the drawbacks of crypto kitties and countermeasures to overcome them.**

***Index Terms*—Smart contracts, Crypto kitties, Non-fungible tokens, Solidity, Ethereum, Genetic algorithm.**

I. Introduction

A. Background

One of the most exceptional technologies that surfaced in late 2017 is the blockchain system [1]. This technology gained popularity nine years after the release of Satoshi Nakamoto's Bitcoin whitepaper [2]. Bitcoin, initially investigated this area for a payment application. However, Ethereum attempts to actualize the space created by "smart contracts beyond the payment process." Smart contracts are open-source programs that execute automatically without the intervention of any centralized authority [3]. The Ethereum platform, often known as Blockchain 2.0, highly motivated the construction of DApps backed by smart contracts [4], [5].

Blockchain technology has opened up a new approach to creating digital scarcity, and perhaps, new types of market value are created due to the advancements [6]. This idea has found practical realization in several digital projects on the blockchain. For example, projects such as Crypto kitties, Crypto punks [7], Care Bears, and Crypto apes have initiated a boom of NFTs on the art marketplace. One of the most important goals of permissionless blockchain technology and smart contract as an application is to ensure that an economic system is transparent and fair. This is uncertain for smart contracts applications but may be true for payment applications such as bitcoin and cryptocurrency.

For the fairness of smart contracts, two aspects need to be considered in the shadow. The first is the effect of an autonomous system, and the other is the liability of the programming code. Users may find it challenging to handle their assets and strategies and comprehend how their financial transactions are carried out fairly if they employ autonomous execution. The users are requested to trust the smart contract's code. But ordinary people find it difficult to comprehend code written in programming languages such as solidity, vyper, etc.

At the time of framing this article, we do not have a good measure to determine whether a specific smart contract or application is fair or not. Therefore, though discussing the integrity of smart contracts is an extensive investigation, it is worthwhile to investigate the underlying causes of smart contract inequity. This direction will serve as the foundation for such evaluation standards.

B. Contributions of this paper

The main contributions of this manuscript are summarized as follow:

1) This paper highlights the potential unfairness of the market created by a worldwide famous application called crypto kitties. According to some estimates, the impact of crypto kitties is worth more than 40 million. Thus, the existence of possible unfairness may raise concerns about the site's credibility as a crypto-asset exchange.
2) In particular, we focus on the breeding process, which is used to generate ERC721 tokens in crypto kitties. In this game, an ERC721 token is a kitty [8]. We assume the purpose of this game for each player is to earn Ether by swapping tokens and having fun with the kitty. The gene algorithm in this game determines the qualities of a freshly born kitten, an ERC-721 coin.

As a consequence of our research, we discovered that crypto kitties does not satisfy certain conditions to employ fairness in the market. The gene determination algorithm lacks qualified randomness, and it has a significant impact on the character determination of a newborn kitten. It is a source of knowledge asymmetry. Only someone aware of the nature of random function can predict the traits of a new kitty. We discovered that individuals who are aware of the bias and can purchase kittens that give birth to valuable kittens earn more profit in the form of Ether. This fact contradicts the fairness of opportunities provided to the users to gain profit. As a

countermeasure, in this paper, we propose an algorithm that incorporates randomness to alleviate the predictability of child genes. The rest of the paper is organized as follows;

Literature review of the previously designed data aggregation models are described in Section II. Section III represents the related preliminaries used throughout the paper. The detailed construction of the proposed model is illustrated in Section IV. Further, we elaborate the experimental analysis in Section V. Finally, we conclude the proposed model with future work in Section VI.

II. Related literature

Alesha Serada et al. [9] looked at crypto kitties as a case study to explore how blockchain will influence game creation in the future. First, they looked into the connection between token ownership and crypto kittie's value construction. Next, they contend with the various aspects of the gaming economy that make it unsustainable. The authors demonstrated the reasons behind the fall in kitty's worth and the value of Gen0, which can not be produced by breeding. They also indicated that higher GAS transaction costs could stifle new user participation.

Kentaro Sako et al. [10] emphasized the importance of fairness in an open and unrestricted market. They highlighted the various unfair factors exercised by crypto kitties. For example, the authors claimed that persons fluent in the Solidity programming language have a better probability of profiting than those unable to forecast the behavior of kitty generation methods. They also proposed countermeasures to reduce the unfairness caused by the market of crypto kitties.

Charlotte et al. [11] discussed the idea of trust without trust in blockchain technology. The authors questioned whether parties might conduct business with one another without relying on officially sanctioned confidence. The writers clearly articulated the need for users to test the legitimacy of claims made by Dapps. They concentrated on a Dapp called crypto kitties and questioned its decentralized aspect. Charlotte emphasizes that it is a flaw that some people can deceive others into carrying out a dishonest commitment.

Alesha Serada demonstrated the significance of 'vintage' for community players in the online crypto games. The author accessed the influence of the label 'vintage' in the early months of 2018 by studying the application of crypto kitties. The author concludes that crypto kitty failed to acquire enormous market value despite gaining explosive popularity due to breeding [12].

Shang Gao et al. [13] discovered the reasons behind the user's intention of using blockchain-based games. Perceived practicality, ease of use, fun, and trust were the vital determinants for the research model. On the other hand, subjective norm had no positive effect on the user's performance expectancy.

III. Preliminaries

This paper aims to bring a fair view to all the players of a blockchain game, crypto kitties irrespective of ETH in their wallet and their ability to comprehend solidity. Furthermore, the proposed methodology increases randomness in the gene determination algorithm used for breeding.

A. Blockchain

Blockchain is a database often used as a ledger for cryptocurrency transactions. Decentralization, censorship-free, immutability, transparency, and anonymity are some of the unique features of Blockchain. A blockchain is made up of a list of blocks. Transactions, a timestamp, a prior hash, and a nonce are included in each block. A transaction mainly consists of three parts: a sender, a recipient, and a value.

Users of the blockchain network submit potential transactions via various software, including desktop applications, smartphone applications, digital wallets, and web services [14]. These transactions are sent to a node or nodes within the blockchain network. Subsequently, the submitted transactions are propagated to the rest of the network's nodes. A pending transaction must wait in a queue until it is published to the blockchain by a publishing node after being broadcasted among nodes. When a publishing node publishes a block, transactions are appended to the blockchain.

B. Smart contracts

Smart contracts are executed on a blockchain when predefined conditions are met. Ethereum is the first to implement smart contracts. They're used to automate the execution so that all participants can be positive of the conclusion without any intermediaries or wastage of time. They can also automate a workflow, starting when certain circumstances are satisfied.

C. Crypto kitties

Crypto kitties are among the most well-known blockchain-based games on Ethereum [15]. Axiom Zen created this game in 2017. Fig. 1 shows the overview of crypto kitties. In this game, users trade ERC721 tokens using the native coin of Ethereum, ether. An ERC721 is a non-fungible token. These tokens are one of a kind with specific properties. The value of each ERC721 token depreciates over time. There is an ID, a gene, and a generation for each cat. The ID of a kitten is assigned in chronological order of birth, and the gene that determines the kitty's appearance is generated via a Solidity algorithm. A child kitty's generation is one greater than the parent kittens' generation. The blockchain stores not only the transactions but the data of these kitties. Smart contracts handle all the trades and breeding in this game as the source code is written in solidity.

There are two ways to obtain a kitty; one is winning an auction and the gene determination algorithm creates the other. The user must choose parent kittens as input to the algorithm to create a new kitty. One parent kitties can be one of his cats or a kitty he got in a rental auction. He can get a baby kitty after picking parent kitties. Thus, this process is known as breeding. A kitten can be either a matron or a sire because it has no gender. The gene and generation of a baby kitten are determined through breeding.

D. Crypto kitty market analysis

A fair market should adhere to the requirements that safeguard the vulnerable. First, it must be impossible to defraud people to make money. The knowledge asymmetry, which allows some people to earn a higher profit than others, must remain relatively small. Finally, all players must be treated equally in the trading environment. The same set of rules must apply to Crypto kitties. In crypto kitties, a way to earn Ether is to get and sell a high-value kitty. All players should get equal chances to own precious kitties for this game to be fair. This paper focuses on the unfair aspect of breeding. So, an unfair practice could include winning the kitty at the auction without obeying the rules or gaining it by manipulating the breeding algorithm. CryptoKitties must prohibit both actions.

Crypto kitties should essentially provide answers to specific questions such as how a new kitty is created and what kind of kitty is traded at what price, regardless of a player's eloquence in Solidity. Again, a user can obtain a kitty by auction or breeding. For breeding, a gene determination algorithm reveals the creation of a kitty. If a player learns the game's mechanism, he will determine which kitten he should receive and which kitties he should choose as parents to gain the most profit. As a result, his decision is influenced by how well he understands the game. Hence, we define the weak as players who have a limited amount of Ethereum and cannot comprehend Solidity.

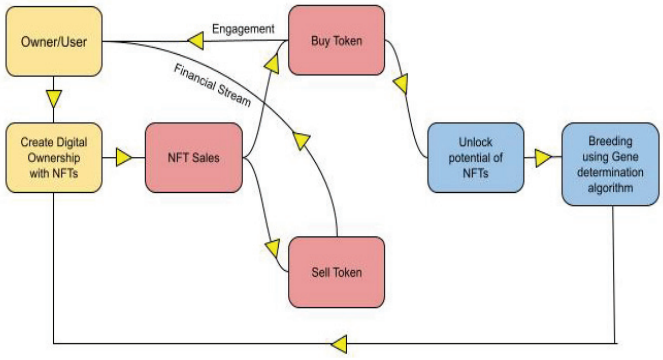

Fig. 1: Overview of crypto kitties

IV. Proposed Model

This section demonstrates the proposed gene determination algorithm that builds the value of tokens to be traded in the market. A gene is a 256-bit unsigned number that defines the kitty's appearance. A gene array of length 16 is considered in this algorithm. This value is classified into eight categories. Each group has two cells; the first two are group 0, the next two are group 1, etc. Each pair displays a different aspect of the kitty's appearance.

The algorithm uses the hash value on the Ethereum blockchain recognized as the target block. A baby gene is dependent on its parents' genes and the target block's hash value. The genes of all kitties are available on the blockchain. The target block is the one that is issued when a matron kitty regains her fertility. Specifically, the product of the variable, which stores the frequency of block creation and the dame's kitty breeding period, results in the blocks issued when she can reproduce again. The information about the breeding period is available on the official website of crypto kitties. By computing the hash value of the target block, one can easily predict a baby gene. The demand for parent cats is high because the outcome of the gene finding algorithm is foreseeable, and only the wealthy can afford them.

A. Working

Fig. 2 illustrates the systems' overview and solution to mitigate the above problem by adding external randomness to the gene determination algorithm. This method implements the genetic algorithm with a discrete crossover operator to produce single offspring. The genes from the parents are selected depending upon the random real number. The mode of the joint input of the users creates this 8-bit random number. The output remains unpredictable as all the users can not predict the information. Further, a small percentage of randomness is deployed to this output by using the timestamp value of the block.

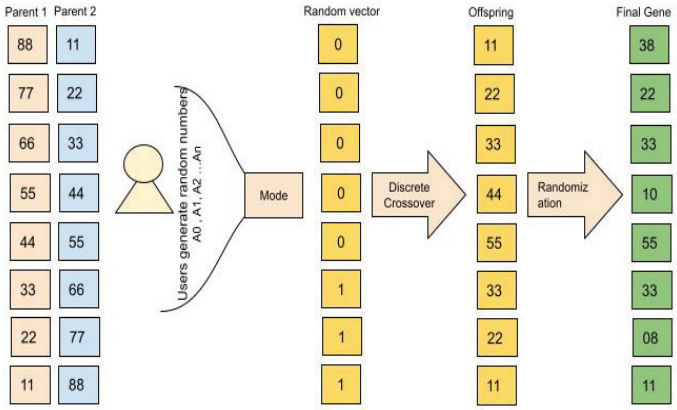

Fig. 2: Overview of counter measure

V. Experimental analysis

To assess the proposed system's effectiveness, we have deployed the smart contracts written in solidity are on the ropsten testnet Ethereum network using the truffle framework. We have tested the proposed functionality successfully. All function calls can be viewed using the etherscan, a blockchain explorer for ropsten to verify the transactions and cost of execution. Fig. 3 shows the implementation of the breeding using the proposed gene determination algorithm.

Fig. 4 illustrates the transaction details of the breeding operation between two kittens. This is a snapshot of a meta mask wallet displaying the information about cumulative gas incurred.

Fig. 3: Breeding operation between 1^{st} and 2^{nd} kitty

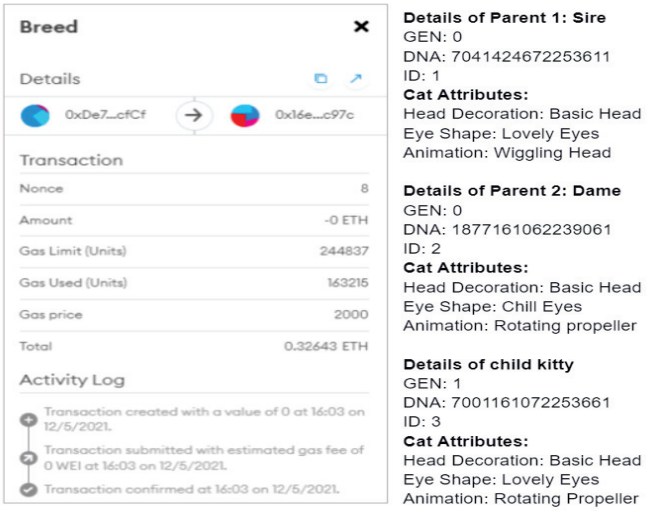

Fig. 4: Metamask snapshot of the breeding

VI. Conclusion and Future work

This paper concludes that the crypto kitty does not provide a fair market for all users. Furthermore, we discovered that the gene determination algorithm depends on the target block's hash value which is easily predictable by the player familiar with solidity. Players can have a significant advantage if they are aware of this bias. To mitigate the unfairness, we have proposed a countermeasure. The proposed solution adds randomness to the gene determination algorithm by taking the input from the users.

We aim to extend this work towards the transaction and breeding fee. Higher transaction fees can be an obstacle for an average user. For example, a user pays Ether in exchange for a kitty. Besides, the current breeding fee is 0.008 ETH. This limits the action count for some players. Therefore, they have limited opportunities to own good kitties and earn profit compared to rich people, and thereby we will propose a countermeasure to reduce breeding fees.

Acknowledgements

This research work is supported by Indian Institute of Technology (ISM), Dhanbad, Govt. of India. The authors wish to express their gratitude and heartiest thanks to the Department of Computer Science & Engineering, Indian Institute of Technology (ISM), Dhanbad, India for providing their research support.

References

[1] Nofer, Michael, Peter Gomber, Oliver Hinz, and Dirk Schiereck. "Blockchain." Business & Information Systems Engineering 59, no. 3 (2017): 183-187.
[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.
[3] Mohanta, Bhabendu Kumar, Soumyashree S. Panda, and Debasish Jena. "An overview of smart contract and use cases in blockchain technology." In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-4. IEEE, 2018.
[4] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper 3, no. 37 (2014).
[5] Cai, Wei, Zehua Wang, Jason B. Ernst, Zhen Hong, Chen Feng, and Victor CM Leung. "Decentralized applications: The blockchain-empowered software system." IEEE Access 6 (2018): 53019-53033.
[6] Lehdonvirta, Vili, and Edward Castronova. Virtual economies: Design and analysis. Mit Press, 2014.
[7] Dowling, Michael. "Is non-fungible token pricing driven by cryptocurrencies?." Finance Research Letters 44 (2022): 102097.
[8] Wang, Qin, Rujia Li, Qi Wang, and Shiping Chen. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." arXiv preprint arXiv:2105.07447 (2021).
[9] Serada, Alesja, Tanja Sihvonen, and J. Tuomas Harviainen. "CryptoKitties and the new ludic economy: how blockchain introduces value, ownership, and scarcity in digital gaming." Games and Culture 16, no. 4 (2021): 457-480.
[10] Sako, Kentaro, Shin'ichiro Matsuo, and Sachin Meier. "Fairness in ERC token markets: A case study of CryptoKitties." In International Conference on Financial Cryptography and Data Security, pp. 595-610. Springer, Berlin, Heidelberg, 2021.
[11] Ducuing, Charlotte. "How to make sure my cryptokitties are here forever? The complementary roles of blockchain and the law to bring trust." European Journal of Risk Regulation 10, no. 2 (2019): 315-329.
[12] Ducuing, Charlotte. "How to make sure my cryptokitties are here forever? The complementary roles of blockchain and the law to bring trust." European Journal of Risk Regulation 10.2 (2019): 315-329.
[13] Gao, Shang, and Ying Li. "An empirical study on the adoption of blockchain-based games from users' perspectives." The Electronic Library (2021).
[14] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." arXiv preprint arXiv:1906.11078 (2019).
[15] Evans, Tonya M. "Cryptokitties, cryptography, and copyright." AIPLA QJ 47 (2019): 219.