CRYPTOKITTIES

Abhishek Singhal
RIT2015016

Ayush Agarwal
RIT2015036

Siddharth Acharya
RIT2015040

Anurag kr kushwaha
RIT2015058

What is cryptokitties ??

- **CryptoKitties** is a blockchain based virtual game developed by Axiom Zen that allows players to purchase, collect, breed and sell various types of virtual cats.
- It represents one of the earliest attempts to deploy blockchain technology for recreational and leisurely purposes.
- The game's popularity in December 2017 congested the Ethereum network, causing for it to reach an all-time high in transactions and slow down significantly.

What's the big deal about Cryptokitties?

- Since its launch in November, CryptoKitties app has reportedly seen $23 million worth of ether spent in buying and trading various unique digital cats on its platform. ($12 million till Dec 9th)

- The decentralized app became so popular that it slowed down the average transaction time on the Ethereum network, sparking conversation on online forums about the necessary growing pains the network has to endure as developers tackle scalability issues.
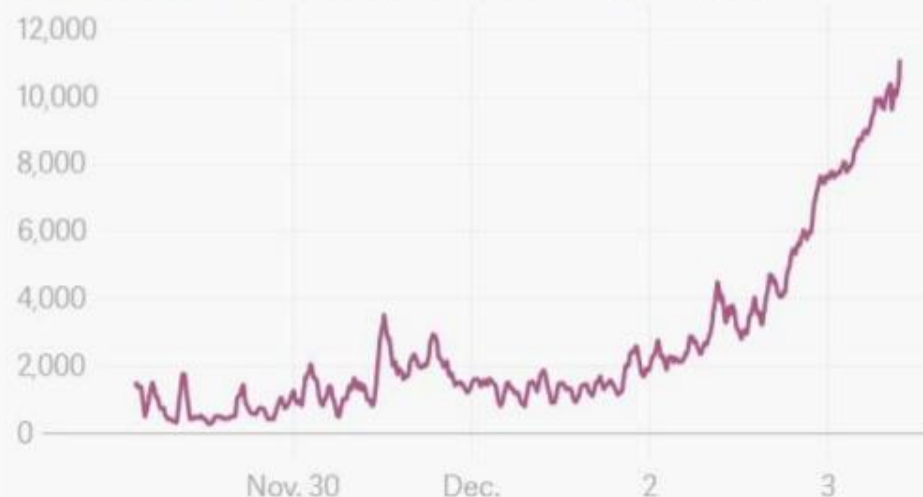
CATS RULE THE BLOCKCHAIN, TOO

The ethereum network is getting jammed up because people are rushing to buy cartoon cats on its blockchain

By Joon Ian Wong | December 04, 2017

12% of all transactions on the ETH in 5 days

Pending ethereum transactions after CryptoKitties' release

Ethereum smart contract address	Proportion of total transactions
0x06012c8cf97bead5deae237070f9587f8e7a266d (CryptoKitties)	11.77%
0x8d12a197cb00d4747a1fe03395095ce2a5cc6819 (EtherDelta)	8.85
0xb1690c08e213a35ed9bab7b318de14420fb57d8c	8.28
0x86fa049857e0209aa7d9e616f7eb3b3b78ecfdb0	1.6
0x7727e5113d1d161373623e5f49fd568b4f543a9e	1.26
0x4e0603e2a27a30480e5e3a4fe548e29ef12f64be	1.21
0x70faa28a6b8d6829a4b1e649d26ec9a2a39ba413 (Shapeshift)	0.64
0xd26114cd6ee289accf82350c8d8487fedb8a0c07	0.57
0x6733d909e10ddedb8d6181b213de32a30ceac7ed	0.38
0x6d5cac36c1ae39f41d52393b7a425d0a610ad9f2	0.36

Source: ETH Gas Station

8

Let's look at how many sales have been made per day:
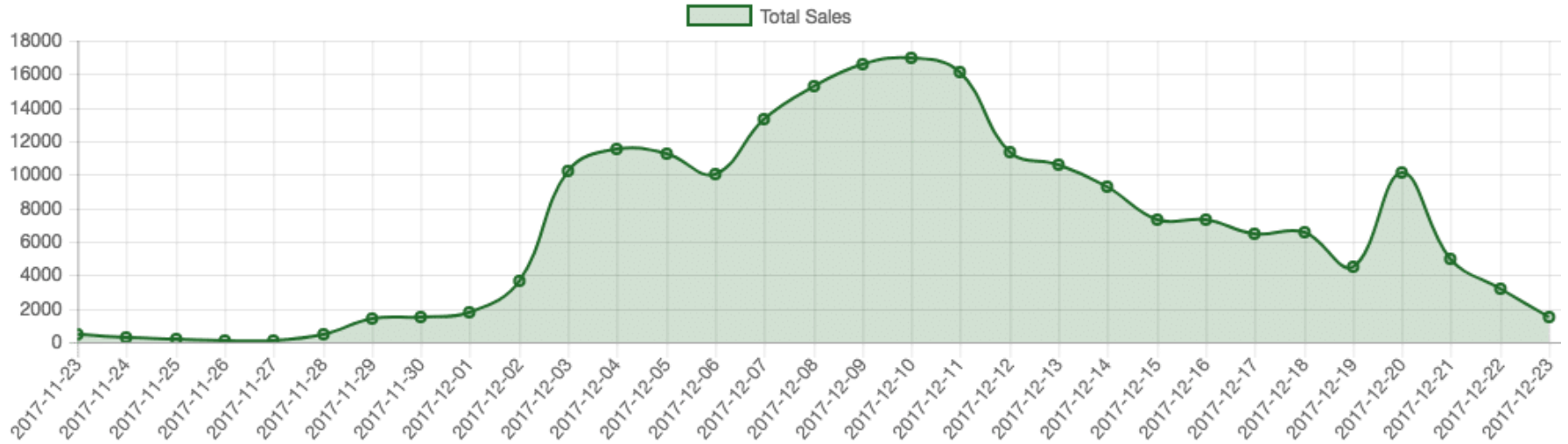
How to Buy CryptoKitties

Before you get started with anything there are three things that you need:

- Chrome or Firefox Browser.

- The Metamask wallet.

- Ether in your Metamask wallet.

That's really all that you need to get started.

Once you have these things sorted out, buying the kitties is very straightforward.

- Go to the Cryptokitties Marketplace.

- Once you are in, this is what you will see:

81,796 kitties

Filter kitties

🏷 For sale Ξ 0.0459

🏷 For sale Ξ 0.0250

🏷 For sale Ξ 0.0646

🏷 For sale Ξ 0.0947

Kitty 394794 · Gen 4 · Swift
♡ 0

Kitty 394787 · Gen 2 · Swift
♡ 1

Kitty 394781 · Gen 2 · Swift
♡ 1

Kitty 394773 · Gen 4 · Swift
♡ 2

🏷 For sale Ξ 0.0495

🏷 For sale Ξ 0.0998

🏷 For sale Ξ 0.0198

New

🏷 For sale Ξ 0.6896

Kitty 394772 · Gen 5 · Swift

Kitty 394765 · Gen 3 · Swift

Kitty 394760 · Gen 9 · Snappy

Kitty 394749 · Gen 0 · Fast

What actually are the cats we are buying?

- The kitties are nothing but a struct with lots of variables.

  - **struct Kitty {**
    - **uint256 genes;**
    - **uint64 birthTime;**
    - **uint64 cooldownEndBlock;**
    - **uint32 matronId;**
    - **uint32 sireId;**
    - **uint32 siringWithId;**
    - **uint16 cooldownIndex;**
    - **uint16 generation;**
  - **}**

genes	The genetic code of the kitty.
birthTime	The exact timestamp of the kitty's birth.
cooldownEndBlock	The minimum time that a kitty has to wait before it can breed again
matronId	The ID of the cat's mother
sireId	The ID of the cat's father
siringWithId	If the cat isn't pregnant then this is set to 0. However, if pregnant then this is set to the Id of the father
cooldownIndes	How much longer the cat has to wait before it can breed again.
generation	The generation of the cat. The first kitties produced were generation 0

All these variables hold the necessary information about the cats.
This part of the contract also keeps track of the kitty's owner. This is done by:

mapping(uint256 =>address) public kittyIndexToOwner;

Cryptokitty: Behind the Hood

It works on pioneering **ERC-721**, a   non-fungible token protocol.

ERC-721

ERC- Ethereum Requests for Comments
ERC is a set of standards that contains functions a smart contract should implement.

In return, contracts, implementing the standard can be used via a single interface. The best example is ERC-20 standard. All Smart Contracts implementing this standard, by default can be listed to crypto exchanges without any extra technical work.

While ERC-20 is a fungible token, ERC-721 is non-fungible.

Fungible and Non-fungible tokens

Fungible means that something can be replaced by another identical item. In the context of cryptocurrencies, a fungible token is one that is not unique and is perfectly interchangeable with other identical tokens. Eg. Currency or a bag of rice.

Non-fungible tokens, on the other hand, are unique in nature and can be distinguished from each other (think of something like a limited edition baseball card). It is the characteristics of a non-fungible item itself that make it desirable and differentiated. This is necessary in cryptokitties since each cat has different value according to its attributes and rarity.

Breeding Cryptokitties

- Cryptokitties uses the Genetic Algorithm to create a new kitty.

- CryptoKitties uses the crossover mechanism to "sire" a child genome using two parent kitties. This child genome is used to generate a new kitty.

And you can create your own unique Cryptokitties
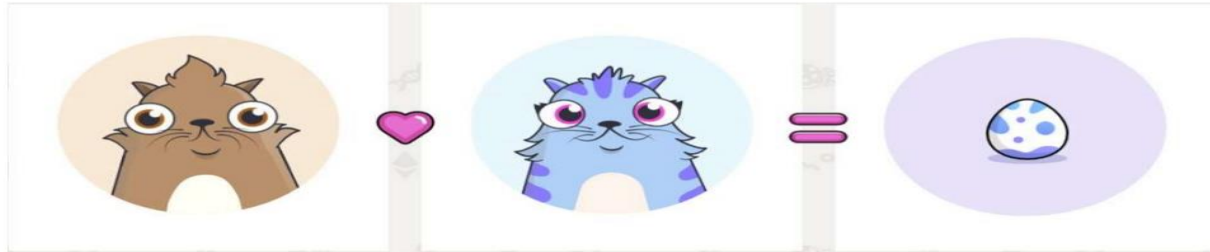
What is Genetic Algorithm?

The genetic algorithm is an optimization technique used to solve nonlinear optimization problems.

It starts with an initial generation of candidate solutions that have been tested against the objective function. The algorithm then generates subsequent solutions from these parent solutions using bio-inspired operators like selection, crossover, and mutation.

- Selection: Selection basically means retaining the best-performing parents from one generation to the next. These well-performing parents are the ones that are preferred for reproduction.

- Crossover: What happens here is that we choose the common variables of the two parents and retain those in the child solution. So using our example:Parent 1:1010011000 Parent2:1001001010 Child: 1000011010 .
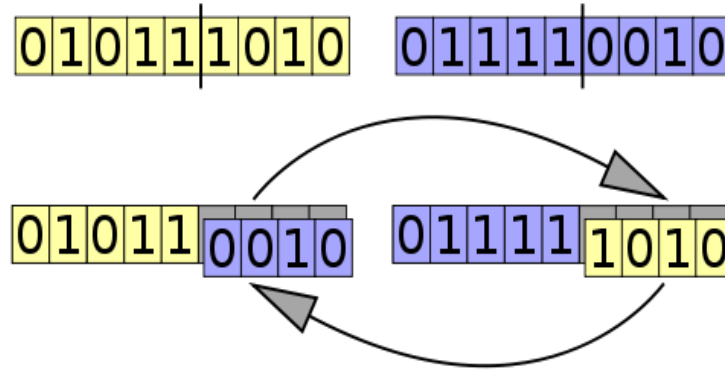
- Mutation: Mutation is when we take a parent and randomly mutate some of their variables to create a child. This is done to make sure that the system can explore other possibilities for optimal solutions.

  Parent: 1010011000 Child: 0101010001 .

Kitty Auctions and Kitty Minting

Auctions: CryptoKitty owners may place their cats available for sire or for sale by selecting a maximum opening bid for siring/selling, a minimum closing bid, and timeframe for the auction. Owners who want to breed their cats may do so by choosing a sire and paying the current descending clock auction bid associated with the sire they want to breed with.

Minting: At launch, 50,000 "Gen 0" cats (colloquially referred to as "Clock Cats") will be stored in a smart contract on the Ethereum blockchain. These Clock Cats will be distributed automatically via smart contract at a rate of one cat every 15 minutes. Each cat will be sold by auction.

Conclusion: The Future is Meow, is it?

And while CryptoKitties is still, by far, the most successful game according to transaction count, it has markedly ebbed since its peak in December. Entering February, some alternatives are attracting higher volumes.

CryptoCountries

Crypto-All Stars

CryptoCelebrities

EtherBots