



Blockchain 101 With CryptoKitties

Andrew Kennedy, Global Food Traceability Center

Andrew Kennedy · Global Food Traceability Center



@foodsafetydad

- MBA, Duke · BA Economics
- Co-Founder of FoodLogiQ
- GFTC Director Emeritus
- IFT's GFTC Vision is to become the global resource and authoritative voice on food traceability.
- IFT Led the FDA FSMA traceability pilot in 2012



Blockchain 101

Why Blockchain Matters:

*“This is not about the technology, **it’s about trust.**”*

David Furlonger, Research Vice President, Gartner

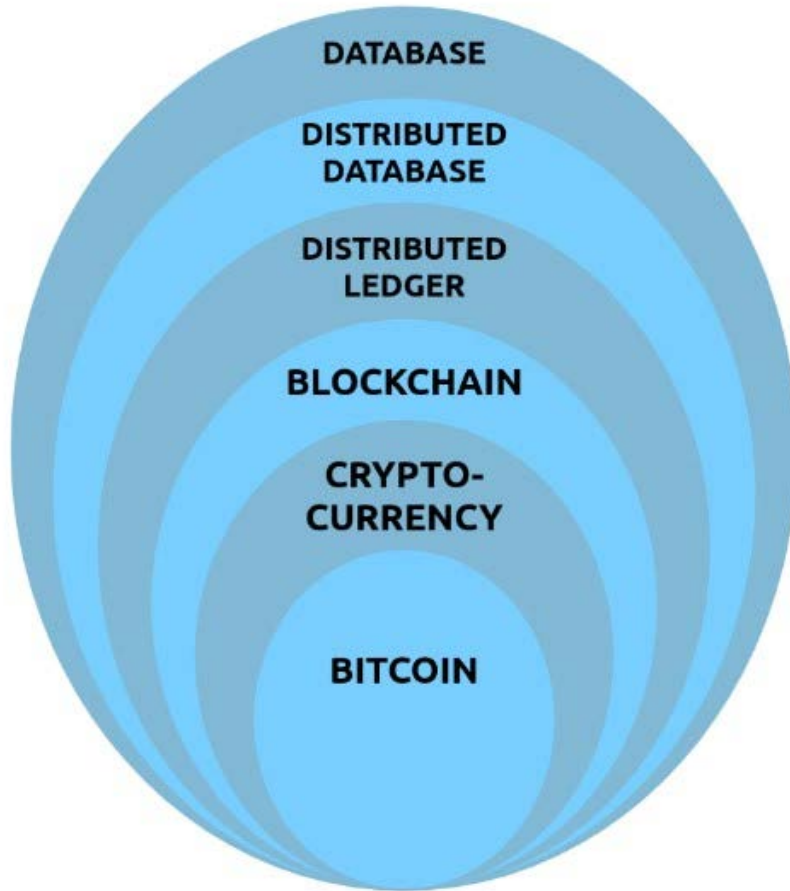
*“The blockchain does one thing: It replaces **third-party trust** with mathematical proof that something happened.”*

Adam Draper, Founder of Boost VC

*“The interesting thing about blockchain is that it has made it possible for humanity to reach a **consensus** about a piece of data without having any authority to dictate it.”*

Jaan Tallinn, Co-Founder Bluemoon

Blockchain Architecture



Source: Sogeti Netherlands 2018

Leading Cryptocurrencies



Bitcoin (BTC)



Ethereum (ETH)



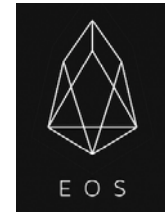
Ripple (XRP)



Bitcoin Cash (BCH)



Litecoin (LTC)



EOS (EOS)

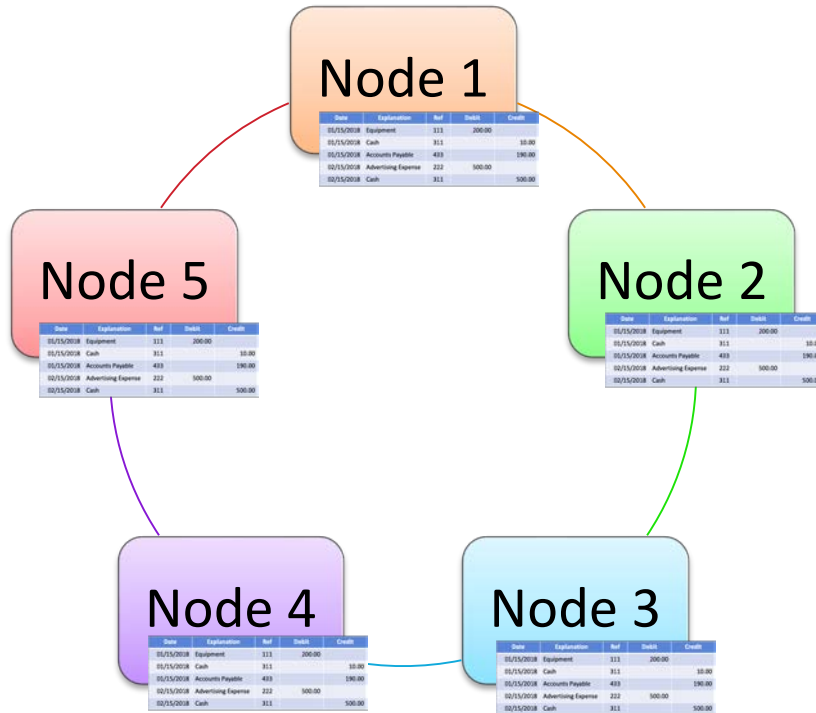
Ledger

Is the principal book or computer file for recording and totaling economic transactions measured in terms of a monetary unit of account by account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account.

Source: <https://en.wikipedia.org/wiki/Ledger>

Date	Explanation	Ref	Debit	Credit
01/15/2018	Equipment	111	200.00	
01/15/2018	Cash	311		10.00
01/15/2018	Accounts Payable	433		190.00
02/15/2018	Advertising Expense	222	500.00	
02/15/2018	Cash	311		500.00

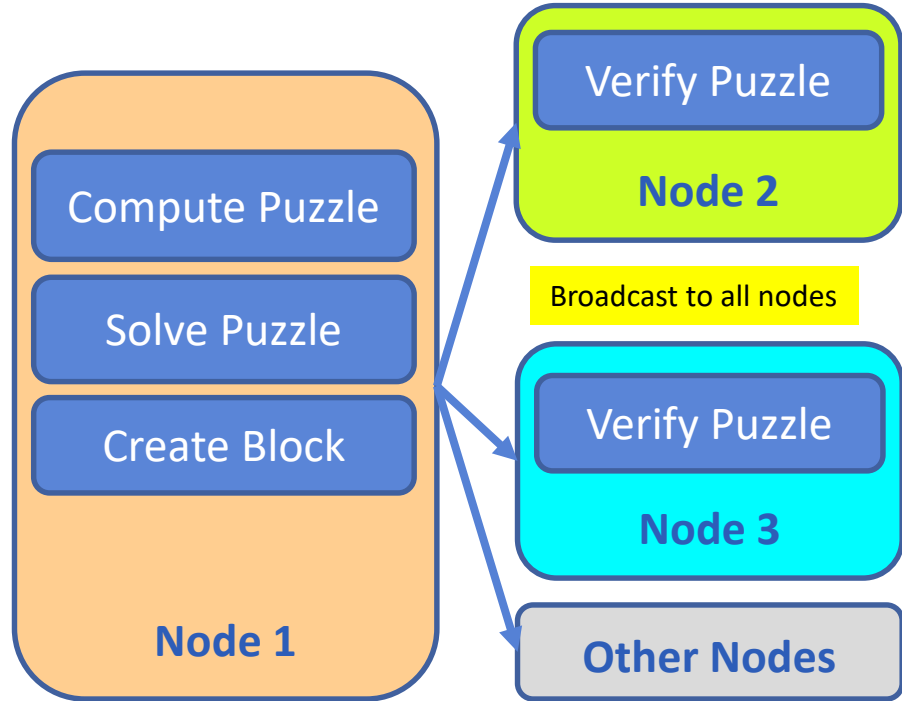
Shared (or Distributed) Ledger



- It is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions.
- There is no central administrator or centralized data storage.
- A peer-to-peer network is required as well as consensus algorithms to ensure replication across nodes is undertaken.
- One form of distributed ledger design is the blockchain system.

https://en.wikipedia.org/wiki/Distributed_ledger

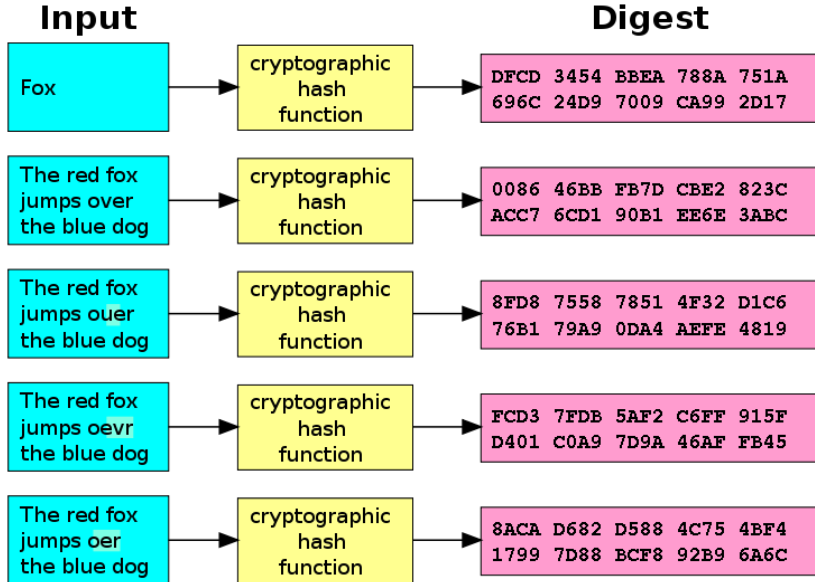
Consensus



- The critical challenge in a distributed ledger is that there is no central authority to determine what to add to the ledger.
- Consensus procedures enable nodes to reach agreement on what to add next to the ledger. Proof of work, proof of stake are examples.

<https://blockgeeks.com/guides/blockchain-consensus/>

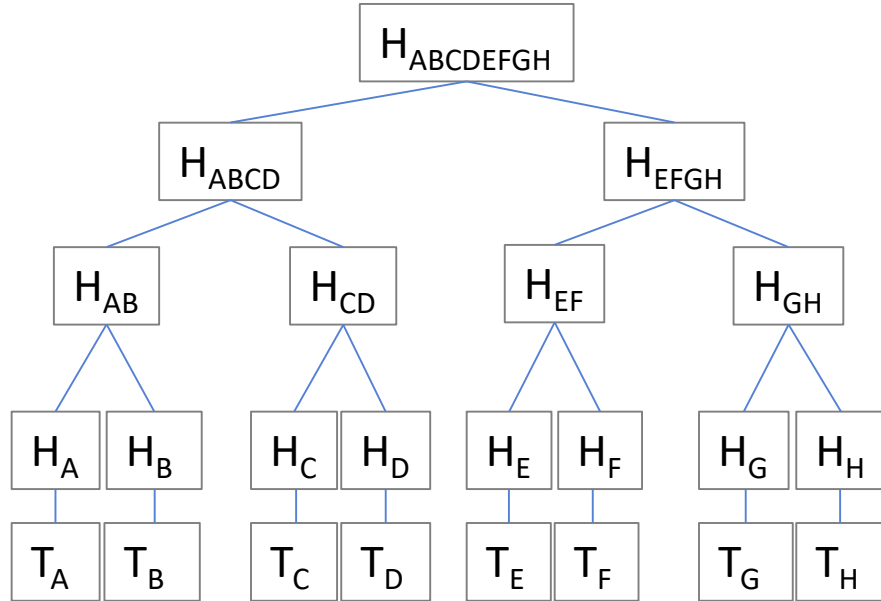
Cryptographic Hash Function



- It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash)
- and is designed to be a one-way function, that is, a function which is infeasible to invert.

Source: https://en.wikipedia.org/wiki/Cryptographic_hash_function

Blocks, Merkle Tree

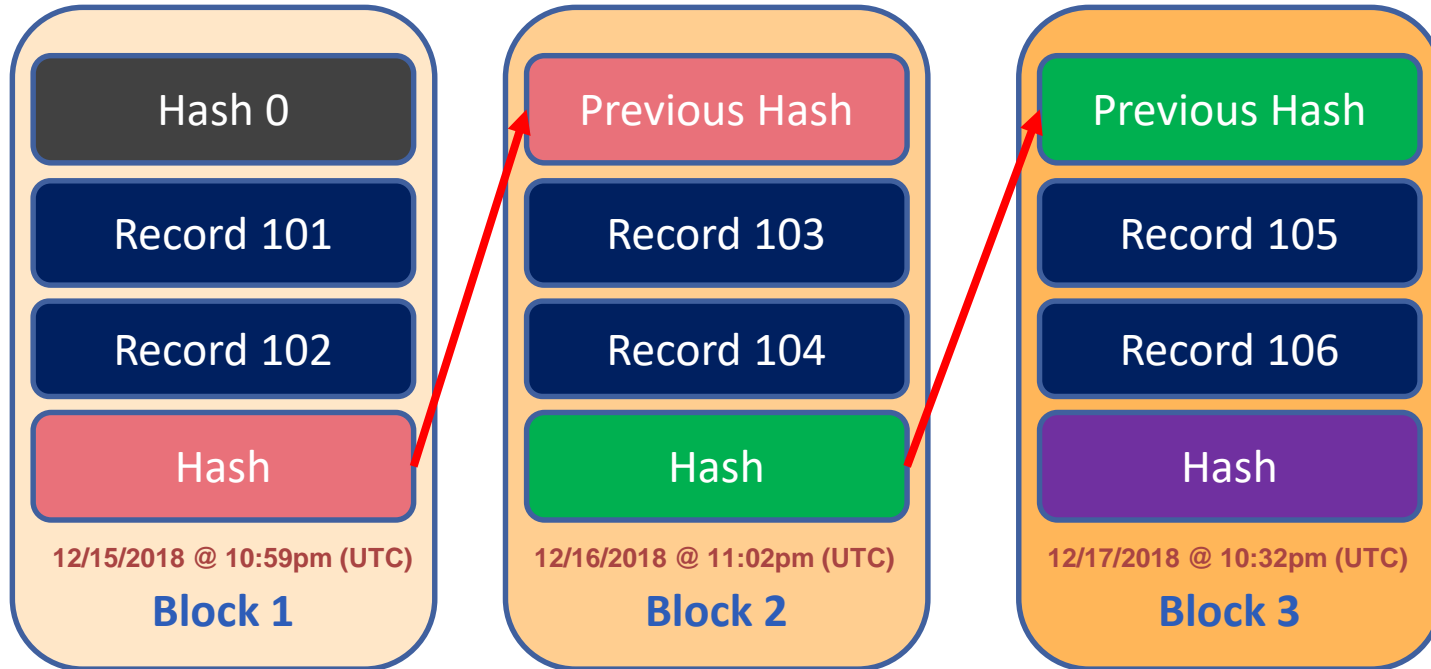


<https://www.investopedia.com/terms/m/merkle-tree.asp>

- Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree;
- Each transaction (example: T_A) is hashed;
- Then each pair of transactions is concatenated and hashed together, and so on until there is one hash for the entire block;
- “T” designates a transaction, “H” is a hash;
- A typical block has over 100 transactions.

Blockchain

- It is a growing list of records, called blocks, which are linked using cryptography.
- Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.



Smart Contract

- Is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.
- Allow the performance of credible transactions without third parties.
- Transactions are trackable and irreversible.
- Aim is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting.

https://en.wikipedia.org/wiki/Smart_contract



<https://www.tradefinanceglobal.com/posts/ethereum-competitor-to-bitcoin/>

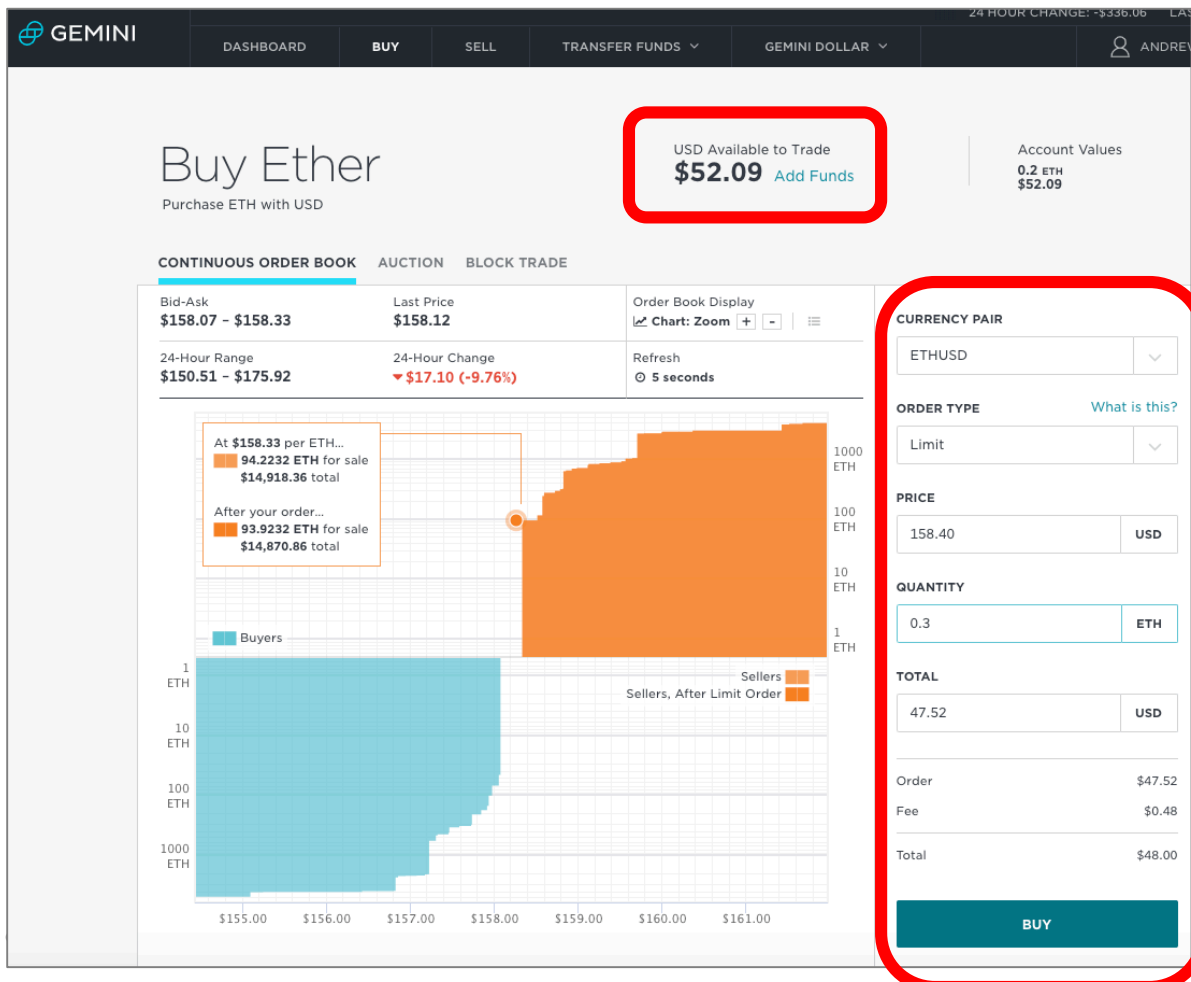
Example Application



CryptoKitties Workflow


1. **Setup Account on Gemini to buy Ethereum (ETH)**
2. **Setup Metamask Wallet (Google Chrome Plugin)**
3. **Setup Account on www.cryptokitties.co**
4. **Wire transfer USD from my bank to Gemini Account**
5. **Transfer ETH from Gemini to a Metamask Wallet**
6. **Purchase Two CryptoKitties**
7. **Breed them**
8. **Now I have Three CryptoKitties!**

Transfer Fiat (USD) from My Bank into Gemini Account and Buy Ether (ETH)



0.3 ETH
@ 158.40 USD
47.52 USD
+ Fee 0.48 USD
Total 48.00 USD

Transfer Ethereum (ETH) to Metamask Wallet



DASHBOARDBUYSELLTRANSFER FUNDS

Withdraw ETH

USD (BANK TRANSFER)USD (WIRE TRANSFER)BTCETHZECBCHLTC

DESTINATION ADDRESS

0x3962A3d0553155E56c858436d638f633a5B


WITHDRAWAL AMOUNT

0.1


MAX


Approximately \$15.79 USD


REVIEW WITHDRAWAL



Main Ethereum Network



Account 1
0x3962...0118



0.1 ETH
\$15.72 USD

DEPOSITSEND

History

You have no transactions



Transaction Details

Earn Interest

Crypto Loan

Sponsored: Nexo - Get instant cash in 40+ currencies using crypto as collateral without selling it. [Get Crypto Loan!](#)

Overview

State Changes

New

Comments

Transaction Hash

Transaction Hash:

0x1c054e98535740e5fb56aa51b6de81676d51b64496da894c014ba5e8bae980c7

Status:

Success

Block:

7504176

35 Block Confirmations

Block # 7504176

TimeStamp:

8 mins ago (Apr-04-2019 09:45:58 PM +UTC)

From:

0xd24400ae8bfebb18ca49be86258a3c749cf46853 (Gemini 1)

0x3962a3d0553155e56c858436d638f633a5bc0118

Destination Address

Value:

0.1 Ether (\$15.98)

Transaction Fee:

0.000147 Ether (\$0.02)

Gas Limit:

90,000

Gas Used by Transaction:

21,000 (23.33%)

Gas Price:

0.000000007 Ether (7 Gwei)

Nonce

Position

524534

28

0.100000 (\$15.98) ETH Transferred
0.000147 (\$0.02) ETH Transaction Fee

Block 7504176

Block 7504177

Hash

Parent Hash

Parent Hash



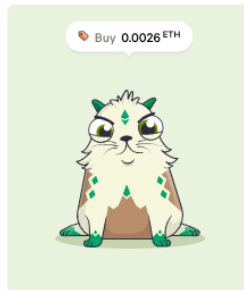
Shop for CryptoKitties

Search

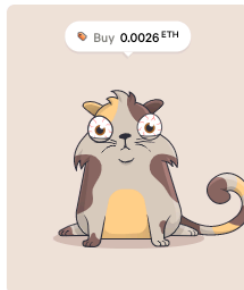
filters

☒ for sale ☐ siring ☐ other

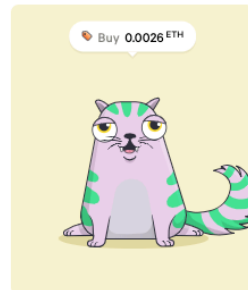
sort by price low to high



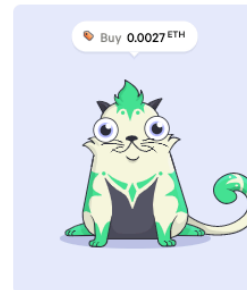
1240788 0
Gen 4 Sluggish



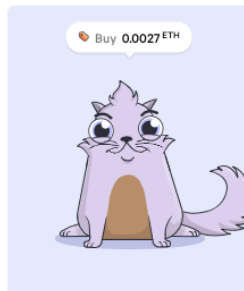
1476161 1
Gen 8 Snappy



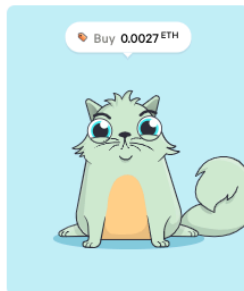
1476175 1
Gen 6 Snappy



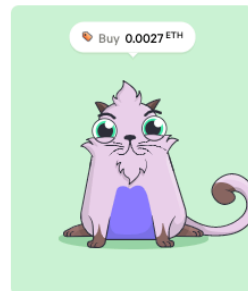
1476343 1
Gen 6 Snappy



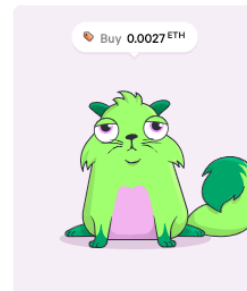
1056548 1
Gen 15 Plodding




1494365 2
Gen 8 Snappy



1494135 3
Gen 7 Snappy



1246939 0
Gen 13 Brisk



Panda Achoobobo

1476343

Gen 6

Snappy Cooldown

Like 1

Make offer

Buy now price

0.0027

Time left

9 days

Buy now

Started at 0.005

Price goes to 0.001

Each Kittie has a Unique Number (Token ID)

Bio i

Ooope. I am Panda Achoobobo and I am better at glaring at the neighbour's cat than you. Try me. My hobbies include catching leprechauns, but only in moderation. This conversation is over.



Hatched by
happybeaver



Birthday
Mar 21 2019

Cattributes i



dahlia
eye colour



bananacream
base colour



highsociety
pattern



selkirk
fur



shale
accent colour



stunned
eye shape



soserious
mouth



swampgreen
highlight colour

Parents

Mother



Father



To Buy a Kittie, the Application Opens Metamask Wallet to Pay For It

Panda Achoobobo

1476343 ⚡ Gen 6 ⌚ Snappy Cooldown


Like 1

Buy now price

Time left

0.0027

9 days



Started at 0.005

Bio

Ooope. I am Panda Achoobobo and I am better at glaring at the neighbour's cat than you. Try me. My hobbies include catching leprechauns, but only in moderation. This conversation is over.

Hatched by happybeaver

Birthday Mar 21 2019

MetaMask Notification

Main Ethereum Network

Account 1 → 0xb169...7d8C

BID

0.002654

\$0.42

DETAILS DATA

GAS FEE 0.000476 \$0.07

AMOUNT + GAS FEE

TOTAL 0.00313 \$0.49

REJECT CONFIRM

Behind the scenes, the following is the actual Blockchain Transaction

[Overview](#) [Internal Transactions](#) [Event Logs \(2\)](#) [State Changes](#) [New](#) [Comments](#)

Transaction Hash: [0x57ec3d69753b26004a54630edf614d1e977ddac99cbc90e1038b4d6e3de7bfaa](#)

Status: Success

Block: [7504479](#) 39 Block Confirmations

TimeStamp: 10 mins ago (Apr-04-2019 10:51:19 PM +UTC)

From: [0x3962a3d0553155e56c858436d638f633a5bc0118](#)

To: [Contract 0xb1690c08e213a35ed9bab7b318de14420fb57d8c](#) (CryptoKitties: Sales Auction) Success
TRANSFER 0.002554046850887347 Ether From 0xb1690c08e213a35ed9b... To 0x9f7064df66ca5856b3af...
TRANSFER 0.00000018749606673 Ether From 0xb1690c08e213a35ed9b... To 0x3962a3d0553155e56c8...

Tokens Transferred: From 0xb1690c08e213a3... To 0x3962a3d0553155... For ERC-721 TokenID [1476343] CK

Value: [0.00265374266581976 Ether](#) (\$0.42)

Transaction Fee: [0.000181524 Ether](#) (\$0.03)

Gas Limit: 158,820

Gas Used by Transaction: 60,508 (38.1%)

Gas Price: [0.000000003 Ether](#) (3 Gwei)

Nonce Position 0 86

Input Data:

#	Name	Type	Data
0	_tokenId	uint256	1476343

tokenId = Cat

You Need Two Kitties to Breed



Kotka Scrummykey

1445288 ⚙ Gen 6 ⌚ Snappy Cooldown

mouse
Owner



Like 0



Make offer

Buy now price

0.003

Buy now

Bio ⓘ

Uh, hi. I'm Kotka Scrummykey. And you are? I have made a mixtape for a duet with Celine Dion, but I'm having a hard time tracking them down. You can help, right? I used to be a Professional Sleeper until I hurt my knees.



Hatched by
mouse



Birthday
Mar 8 2019

Cattributes ⓘ



pearl
highlight colour



icy
accent colour



sapphire
eye colour



amur
pattern



serpent
eye shape



whixtensions
mouth



sphynx
fur



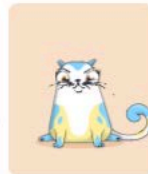
greymatter
base colour

Parents

Mother



Father



Second Transaction

[Overview](#) [Internal Transactions](#) [Event Logs \(2\)](#) [State Changes](#) [Comments](#)

Transaction Hash:

0x95ee9ba8d846df529c05c4291b00b171c0fae4745c9254f4029c116ea2bad45b

Status:

Success

Block:

7504496 2 Block Confirmations

TimeStamp:

30 secs ago (Apr-04-2019 10:56:17 PM +UTC)

From:

0x3962a3d0553155e56c858436d638f633a5bc0118

To:

Contract 0xb1690c08e213a35ed9bab7b318de14420fb57d8c (CryptoKitties: Sales Auction)
 TRANSFER 0.0028875 Ether From 0xb1690c08e213a35ed9b... To 0x7045540552d1fcc2ab1...

Tokens Transferred:

From 0xb1690c08e213a3... To 0x3962a3d0553155... For ERC-721 TokenID [1445288] CK

Value:

0.003 Ether (\$0.47)

Transaction Fee:

0.000125616 Ether (\$0.02)

Gas Limit:

125,815

Gas Used by Transaction:

41,872 (33.28%)

Gas Price:


0.000000003 Ether (3 Gwei)

Nonce

1 73

Input Data:


#	Name	Type	Data
0	_tokenId	uint256	1445288
<i>Decoded input inspired by Canoe Solidity</i>			

Etherscan

Eth: \$157.69 (-4.20%)

HomeBlockchainTokensResourcesMoreSign In

Search by Address / Txhash / Block / Token / Ens

Token CryptoKitties

[CryptoKitties](#) [NFT](#) [Collectibles](#)

[Earn Interest](#) [Crypto Loan](#)

Overview [ERC-721]




Total Supply: 1,508,099 CK

Holders: 73,797 addresses

Profile Summary

Contract: 0x06012c8cf97bead5deae237070f9587f8e7a266d

Official Site: <https://www.cryptokitties.co/>

Social Profiles:   

5 FILTERED BY TOKEN HOLDER

[0x3962a3d0553155e56c858436d638f633a5bc0118](#)

BALANCE



2 CK

TransfersInventoryInfoDEX TradesRead ContractWrite ContractAnalytics

0x3962a3d0553155e56c85...x

A total of 2 tokens

First<Page 1 of 1>Last



[#1476343](#)
CryptoKitties

[#1445288](#)
CryptoKitties

Breed Kitties

These two lovely Kitties will soon be parents!

Dame 🐱

This Kitty will be preppers

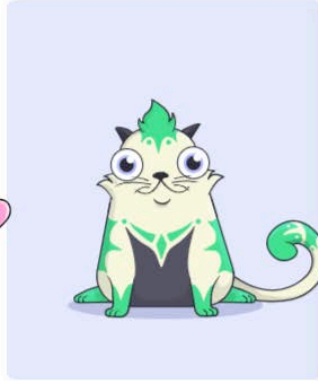


1445288

⌘ Gen 6 🕒 Snappy

Sire 🐱

This Kitty will... you know ;)



1476343

⌘ Gen 6 🕒 Snappy

Birthing fee ⓘ	≡ 0.008
Estimated transaction fee ⓘ	≡ 0.0004
Estimated total	≡ 0.0084

By clicking the button below, your two kitties will breed, and the **offspring** will belong to you once it's born.

Breeding Costs: 0.008 ETH plus fees

MetaMask Notification

Main Ethereum Network

Account 1 → Crypto Kitties

CONTRACT INTERACTION

0.008
\$1.25

DETAILS DATA

GAS FEE 0.00036
\$0.06

AMOUNT + GAS FEE

TOTAL 0.00836
\$1.31

REJECT CONFIRM

Breeding Transaction on Blockchain

Transaction Details

Etherscan - Sponsored slots available. [Book your slot here!](#)

Overview

Event Logs (1)

State Changes

New

Comments

Transaction Hash: [0x04e6265ba830145f12ed5ac898df1faa561897d8e62edd50764cbb462ab44714](#)

Status: Success

Block: [7504579](#) 4 Block Confirmations

TimeStamp: 57 secs ago (Apr-04-2019 11:14:10 PM +UTC)

From: [0x3962a3d0553155e56c858436d638f633a5bc0118](#)

To: Contract [0x06012c8cf97bead5deae237070f9587f8e7a266d](#) (CryptoKitties: Core)

Value: 0.008 Ether (\$1.27)

Transaction Fee: 0.000239955 Ether (\$0.04)

Gas Limit: 119,977

Gas Used by Transaction: 79,985 (66.67%)

Gas Price: 0.000000003 Ether (3 Gwei)

Nonce 2 Position 68

Input Data:

#	Name	Type	Data
0	_matronId	uint256	1445288
1	_sireId	uint256	1476343

Breeding Cost

Parents

My Transaction History

All Filters

Search by Address / Txhash / Block / Token / Ens



Blockchain

Tokens

Resources

More

Sign In



Address 0x3962A3d0553155E56c858436d638f633a5Bc0118



Earn Interest

Crypto Loan

Sponsored:  **Ethereal Virtual Hackathon** - Compete for \$50K in prizes, hosted by Gitcoin + Microsoft [Sign up now!](#)

Overview

Balance: 0.085799349830246913 Ether

Ether Value: \$13.61 (@ \$158.64/ETH)

Token:

1

More Info



Transactions: 4 txns

Transactions

Internal Txns





Erc721 Token Txns

Analytics New

Comments

Latest 4 txns



TxHash	Block	Age	From	To	Value	[TxFee]
0x04e6265ba83014...	7504579	10 mins ago	0x3962a3d0553155...	OUT  CryptoKitties: Core	0.008 Ether	0.000239955
0x95ee9ba8d846df...	7504496	28 mins ago	0x3962a3d0553155...	OUT  CryptoKitties: Sales ...	0.003 Ether	0.000125616
0x57ec3d69753b26...	7504479	33 mins ago	0x3962a3d0553155...	OUT  CryptoKitties: Sales ...	0.002653742665819 Ether	0.000181524
0x1c054e98535740...	7504176	1 hr 38 mins ago	Gemini 1	IN  0x3962a3d0553155...	0.1 Ether	0.000147

The Proud Parents

Kitties

Special Cats

Cat Codex

Collections

New Cat



Loki Fabbear

1508109

♡ 0

⌘ Gen 7 ⌚ Snappy

Sire



Panda Achoobobo

1476343

♡ 1

⌘ Gen 6 ⌚ Snappy

Matron



Kotka Scrummykey

1445288

♡ 0

⌘ Gen 6 ⌚ Snappy

Loki's Transaction, Cattributes, ID and Link to Matron



Loki Fabbear

1508109 X Gen 7 ⌚ Snappy Cooldown

Food Safety Dad (you)
Owner



Like 0



Breed

Sell

Gift

Bio

Good day, I'm Loki Fabbear. Let's cut to the chase. I can whistle any Tom Jones song. It's a weird talent, but it entertains most people. Pffft, whatever.



Hatched by
Food Safety Dad



Birthday
Apr 4 2019

Cattributes



icy
accent colour



amur
pattern



dahlia
eye colour



ragdoll
fur

Event Logs (2)

State Changes New

Comments

0x2fe6241ece12722f12caeecb9bf5baa897423c34bfa505afd07747ec3286b01c

Success

7504621

36 Block Confirmations

10 mins ago (Apr-04-2019 11:23:54 PM +UTC)

0xab5622d7da96c571c6abe08e4b85e462eb666e4f

Contract 0x06012c8cf97bead5deae237070f9587f8e7a266d (CryptoKitties: Core)

TRANSFER 0.008 Ether From 0x06012c8cf97bead5dea... To 0xab5622d7da96c571c6a...

From 0x0000000000000000... To 0x3962a3d0553155... For ERC-721 TokenID [1508109] CK



0 Ether (\$0.00)

0.0029631284139 Ether (\$0.47)

350,000

260,266 (74.36%)

0.000000011385000015 Ether (11.385000015 Gwei)

38333 11

Matron

Nonce Position

Input Data:

#	Name	Type	Data
0	_matronId	uint256	1445288

Querying a Smart Contract on the Blockchain

The screenshot shows the Etherscan website interface for the CryptoKitties token. The top navigation bar includes the Etherscan logo, a search bar, and links for Home, Blockchain, Tokens, Resources, and More. The main header displays the token name 'Token CryptoKitties' and buttons for 'Earn Interest' and 'Crypto Loan'. Below the header, the 'Overview' section for ERC-721 tokens lists the total supply (1,508,113 CK), the number of holders (73,799 addresses), and the number of transfers (3,825,117). The 'Profile Summary' section on the right provides the contract address (0x06012c8cf97bead5dae237070f9587f8e7a266d), the official site (https://www.cryptokitties.co/), and social media profiles. At the bottom, a navigation bar contains links for Transfers, Holders, Inventory, Info, DEX Trades, **Read Contract** (highlighted with a red box), Write Contract, Analytics, and Comments. A '[Reset]' button is located at the bottom right of the page.

Etherscan

Eth: \$158.30 (-1.70%)

Home Blockchain Tokens Resources More Sign In

Token CryptoKitties

Earn Interest Crypto Loan

CryptoKitties NFT Collectibles

Overview [ERC-721]

Total Supply:	1,508,113 CK
Holders:	73,799 addresses
Transfers:	3,825,117

Profile Summary

Contract: 0x06012c8cf97bead5dae237070f9587f8e7a266d

Official Site: https://www.cryptokitties.co/

Social Profiles: [Email] [YouTube] [Twitter]

Transfers Holders Inventory Info DEX Trades **Read Contract** Write Contract Analytics New Comments

[Reset]

Query by tokenID results in a listing of attributes

32. getKitty

_id (uint256)


1508109

Query

isGestating bool, isReady bool, cooldownIndex uint256, nextActionAt uint256, siringWithId uint256, birthTime uint256, genes uint256

[getKitty method Response]

- » isGestating bool : false
- » isReady bool : true
- » cooldownIndex uint256 : 3
- » nextActionAt uint256 : 0
- » siringWithId uint256 : 0
- » birthTime uint256 : 1554420234
- » matronId uint256 : 1445288
- » sireId uint256 : 1476343
- » generation uint256 : 7
- » genes uint256 : 623491275775300058545664179263902970762878246791542975961715931384846415



Loki Fabbear

1508109

Gen 7 Snappy

What else can I do with my cats?



KittyVerse

Take your Kitties to new heights

Your CryptoKitty unlocks a universe of infinite experiences.

You can still breed and collect the CryptoKitties—but now, your favourite Kitty can participate in races, get in a literal catfight, and much more!

KITTYRACE

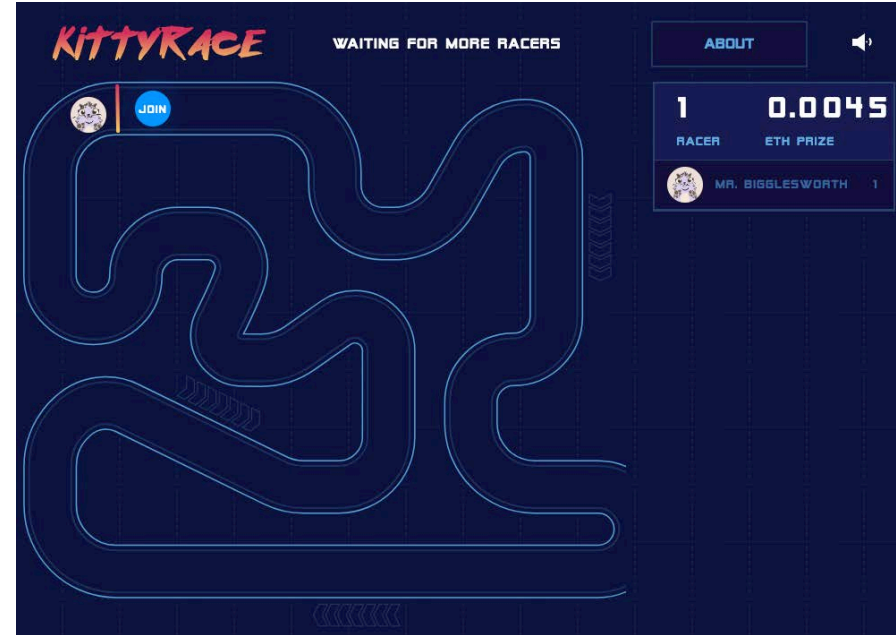
Kitty Race
kittyrace.com

 **KittyHats**

Kitty Hats
kittyhats.co

**KITTY
BATTLES**

Kitty Battles
alpha.kittybattles.io

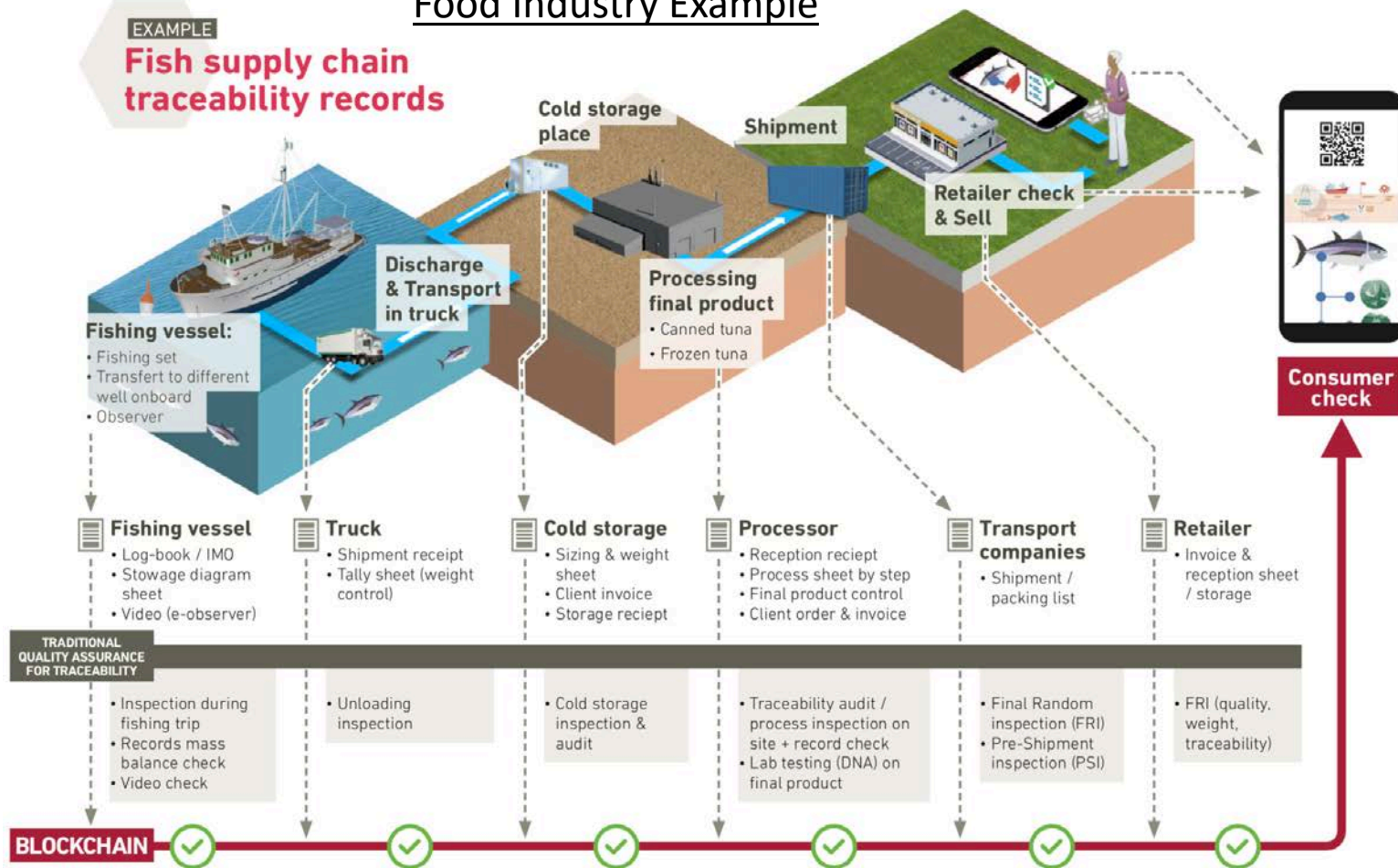


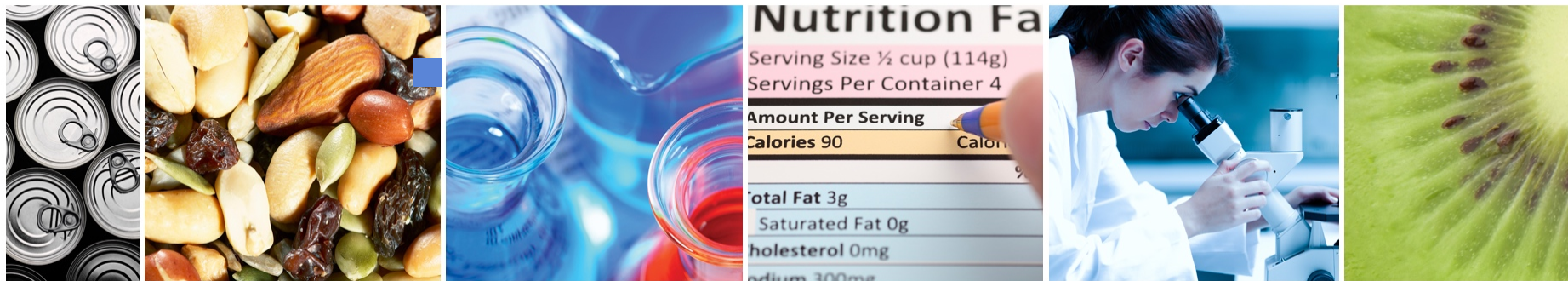
Food Industry Example



EXAMPLE

Fish supply chain traceability records





Blockchain 101 With CryptoKitties

Andrew Kennedy, Global Food Traceability Center


twitter
@foodsafetydad

