CRYPTOCURRENCY

ET AL.

What is Gold Mining

- ***Gold mining*** is the extraction of gold. Gold is a yellow precious metal with an atomic number of 79. It is used in jewelry and decorations and to guarantee the value of currencies. Gold mining is at least 7,000 years old.
- The **work** or mining is accomplished by using hard rock mining, placer mining and recreational approaches to extract the gold. At the end of 2021 it cost about $1,129 to mine one ounce of gold.

What is Bitcoin Mining

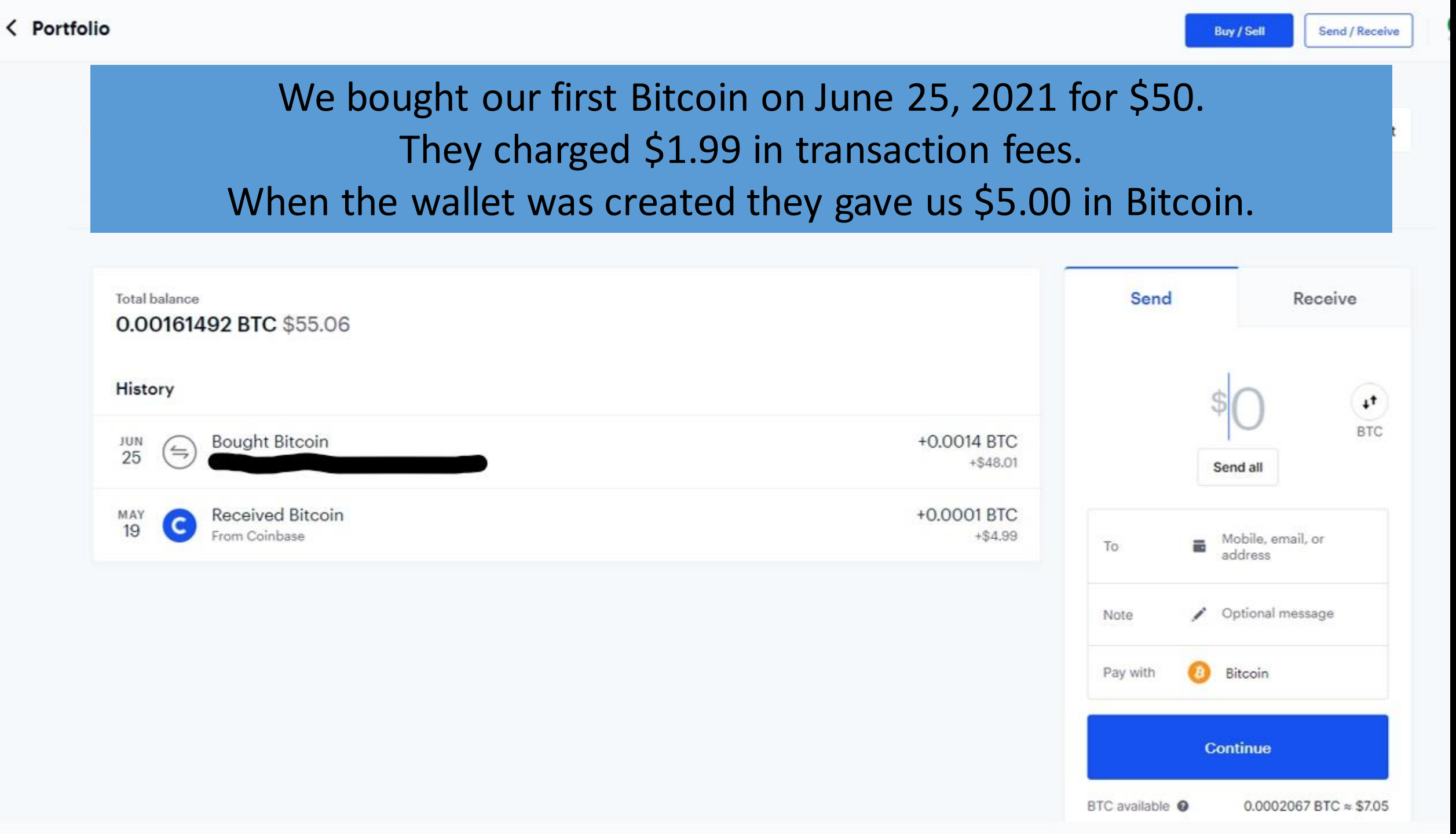
- ***Bitcoin mining*** involves the validating of a block of Bitcoin transactions and then adding the transactions to a distributed ledger.
- The **work** in Bitcoin mining involves **hashing**. Bitcoin miners take the a block of Bitcoin transactions and compute a **hash** with 19 or so leading zeros.
- The miner that generates a hash with 19 zeros gets 6.25 Bitcoins. That is how Bitcoin digital currency is created.
- It costs about $21,000 to mine one Bitcoin in August of 2022 in the US. But that number is all over the place around the world ($1,400 in Kuwait and $246,000 in Venezuela).

Hashing is simple, but computationally intensive

- **Hashing** is simple with computers, but because the block has to have a certain number of leading zeros, the calculation is computationally intensive. It requires trillions and trillions of calculations per second.
- Check out the cost of mining around the world:
  - https://www.forbes.com/advisor/investing/cryptocurrency/is-bitcoin-mining-profitable/

The Bottom Line

- In the Real World
  - Miners dig, blast, smash, rinse and process to obtain gold. The miner gets to keep the gold.
- In the Crypto World
  - Miners calculate a simple math problem involving cryptocurrency transaction over and over until the right answer is found. The miner that gets the right answer receives 6.25 Bitcoins.


Portfolio
Buy / Sell
Send / Receive
We bought our first Bitcoin on June 25, 2021 for $50.
They charged $1.99 in transaction fees.
When the wallet was created they gave us $5.00 in Bitcoin.
Total balance
0.00161492 BTC $55.06
History
JUN 25
Bought Bitcoin
+0.0014 BTC
+$48.01
MAY 19
Received Bitcoin
From Coinbase
+0.0001 BTC
+$4.99
Send
Receive
$0
BTC
Send all
To
Mobile, email, or address
Note
Optional message
Pay with
Bitcoin
Continue
BTC available
0.0002067 BTC ≈ $7.05

Bitcoin #1

▲ $34,715.00

0.00005158 BTC ≈ $1.79

Overview | Account details | Send | Receive | Trade

1D 1W 1M 1Y ALL | Range

1 WEEK	INCOMING	OUTGOING
1 transaction	+ 0.00013733 BTC	+ 0 BTC
Jun 23, 2021 - Jun 30, 2021	$4.75	$0.00

Transactions

PENDING TRANSACTION • 1

Sending BTC — − 0.00008241 BTC
15:33 • 3965j[redacted] — $3.00
Bump fee

JUNE 29, 2021 +$5.01

Received BTC — + 0.00013733 BTC
13:41 • bc1qwy[redacted] — $5.01

Blockchain ART Simulation & Related Concepts

Sean P Sanders
Department of Computer Science

G. Lawrence Sanders
Department of Management Science and Systems
SUNY-Buffalo

BARTS applications were developed by Sean Sanders
spsander@buffalo.com
www.artbarts.com

This material is in part supported by the NSF under grant No. DGE-1754085.

The Bart’s price pattern

The Bart's phenomena is often used to describe the volatility of Bitcoin prices because the pattern looks like the shape of Bart Simpson's head. We selected the name for our simulation before we heard about the Bart's pattern.

Crypto Trading Academy: What are Barts and How They Affect Bitcoin?

“By looking on small frame Bitcoin’s chart, one can identify sudden movements or ‘bump’ in one direction, followed by consolidation and a sudden ‘bump’ to the other direction that ends close to the base price.
This phenomenon can also happen in non-crypto assets, and it has given the name “Barts” because the asset’s price pattern looks like the head’s shape of the iconic Simpsons character, Bart Simpson.”

November 15, 2021

BTC / USD • CRYPTOCURRENCY

Bitcoin to United States Dollar

63,960.40 ↑300.27% +47,980.90 1Y

Nov 15, 9:15:08 PM UTC · Coinbase · Disclaimer

1D 5D 1M 6M YTD 1Y 5Y MAX

Compare to

Ether (ETH / USD)	Litecoin (LTC / USD)	Dogecoin (DOGE / USD)	Cardano (ADA / U
4,574.12	262.38	0.26	2.02
ETH ↑918.64%	LTC ↑320.68%	DOGE ↑9,361.94%	ADA ↑1,91

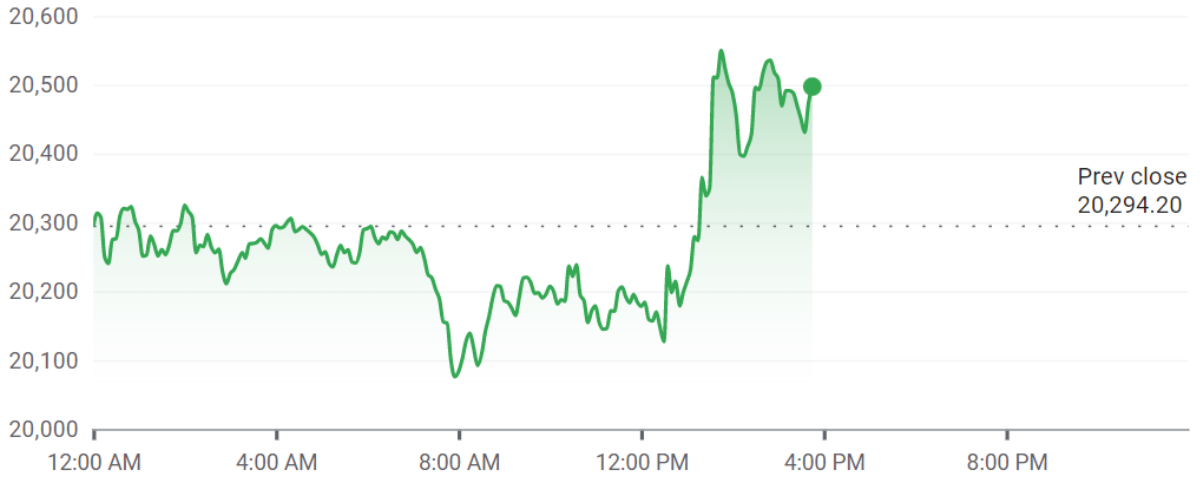
October 28, 2022

Bitcoin to United States Dollar

20,497.10 ↑1.00% +202.90 Today

Oct 28, 3:44:58 PM UTC · Disclaimer

1D 5D 1M 6M YTD 1Y 5Y MAX



Compare to

Ether (ETH / USD)	Litecoin (LTC / USD)	Dogecoin (DOGE / USD)	Cardano (ADA / USD)
1,537.75	54.69	0.0841	0.3940
ETH ↑1.54%	LTC ↓0.26%	DOGE ↑8.91%	ADA ↑1.43%

THE AGENDA

- Introduction
- Mining & Hashing
- BARTS Simulation

Satoshi Nakamoto developed the digital currency Bitcoin

Bitcoin uses blockchain technology to validate and add transactions to a distributed ledger.

Ivan Radic

Who is using Blockchain

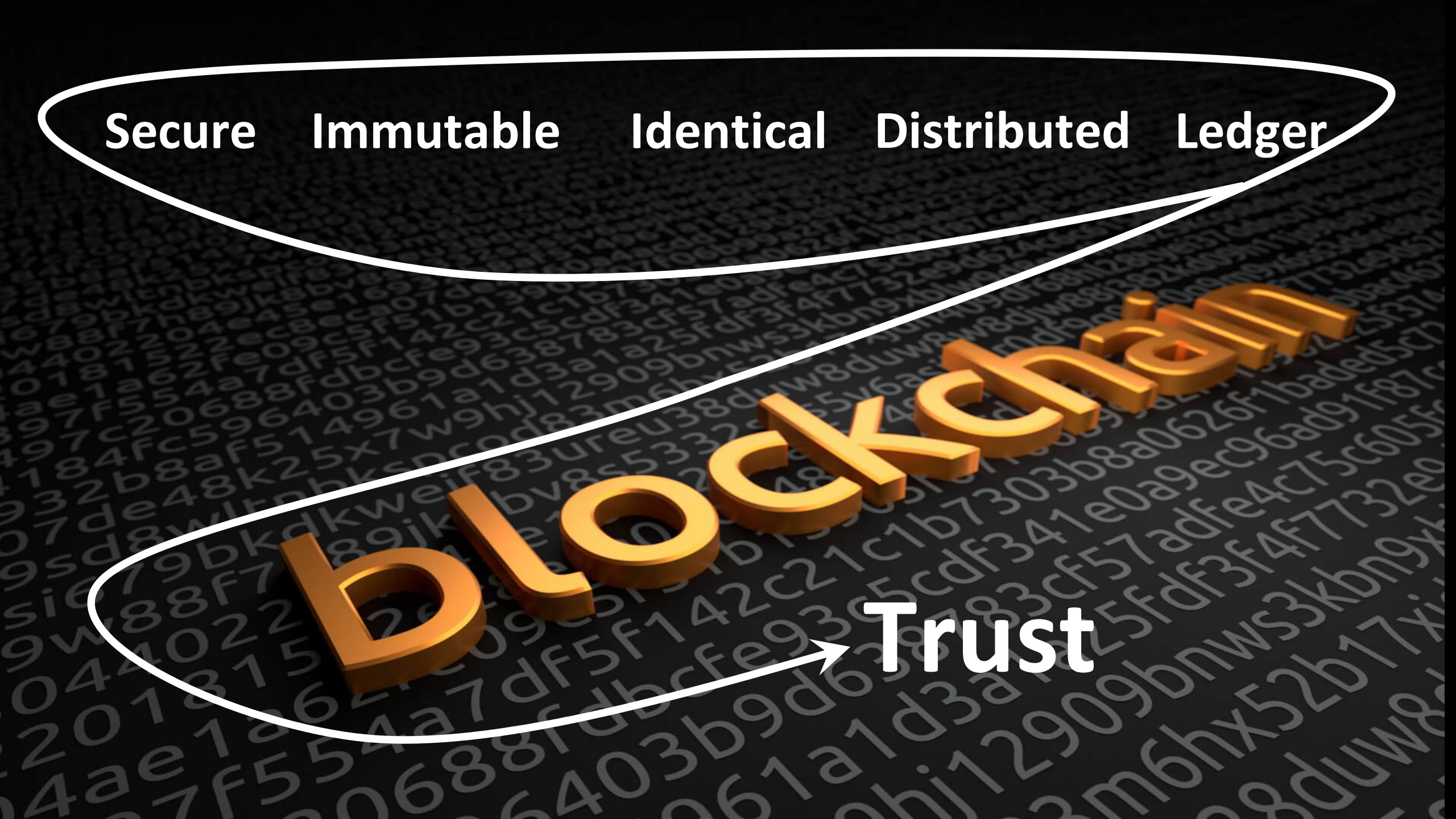
Retail

Government

Healthcare

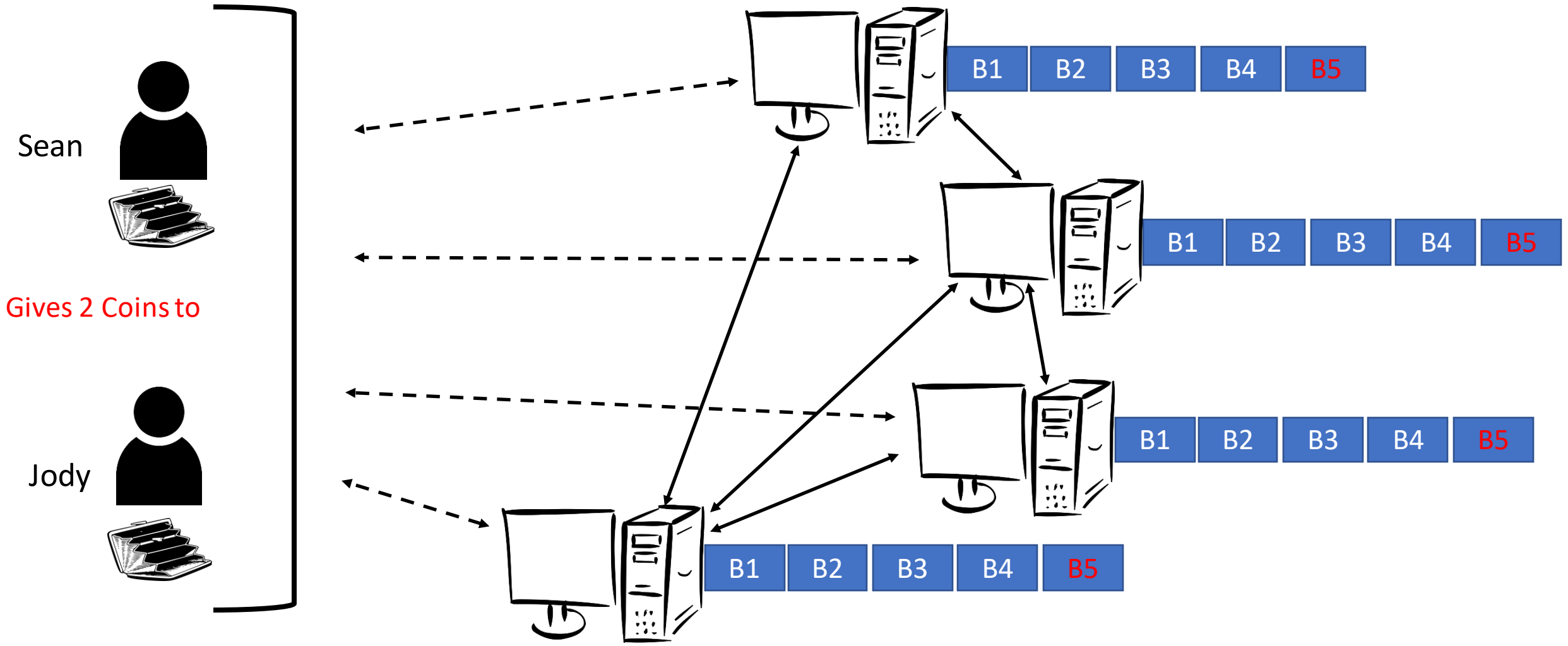
Supply Chain

Financial Institutions


Secure Immutable Identical Distributed Ledger
blockchain
Trust

Blockchain is distributed peer-to-peer append only database

Transactions are secured and authenticated using private and public keys, hashing, and consensus protocols (proof -of-work and proof of stake).



HOW ARE MINING, HASHING AND CRYPTO RELATED

Hashing is used in Bitcoin Mining

Miners try to find a hash, for a group of Bitcoin transaction payments.

The tricky part is that the hash must have a certain number of leading zeros.

Transferring crypto from one wallet to another involves miners solving a hashing problem


Bitcoin miners use application-specific integrated circuit (ASIC) computers designed just for mining Bitcoins

What is **hashing** and a **hash**

- **Hashing** is the process of converting a string of characters into a short fixed-length value. Usually shown in hexadecimal format
- The resulting number is called a **hash** and you cannot reverse engineer back to the original text.
- Bitcoin miners take a 1.5 million character block of about 1,500 Bitcoin transactions and find a **hash** with about 19 or so leading zeros in around 10 minutes using the SHA 256 algorithm.

The SHA 256 hash function always outputs the same length.
It is a 256 bit string represented by 64 hexadecimal characters

SHA 256 Hash algorithm

Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created equal.

Now we are engaged in a great civil war, testing whether that nation, or any nation so conceived and so dedicated, can long endure. We are met on a great battle-field of that war. We have come to dedicate a portion of that field, as a final resting place for those who here gave their lives that that nation might live. It is altogether fitting and proper that we should do this.

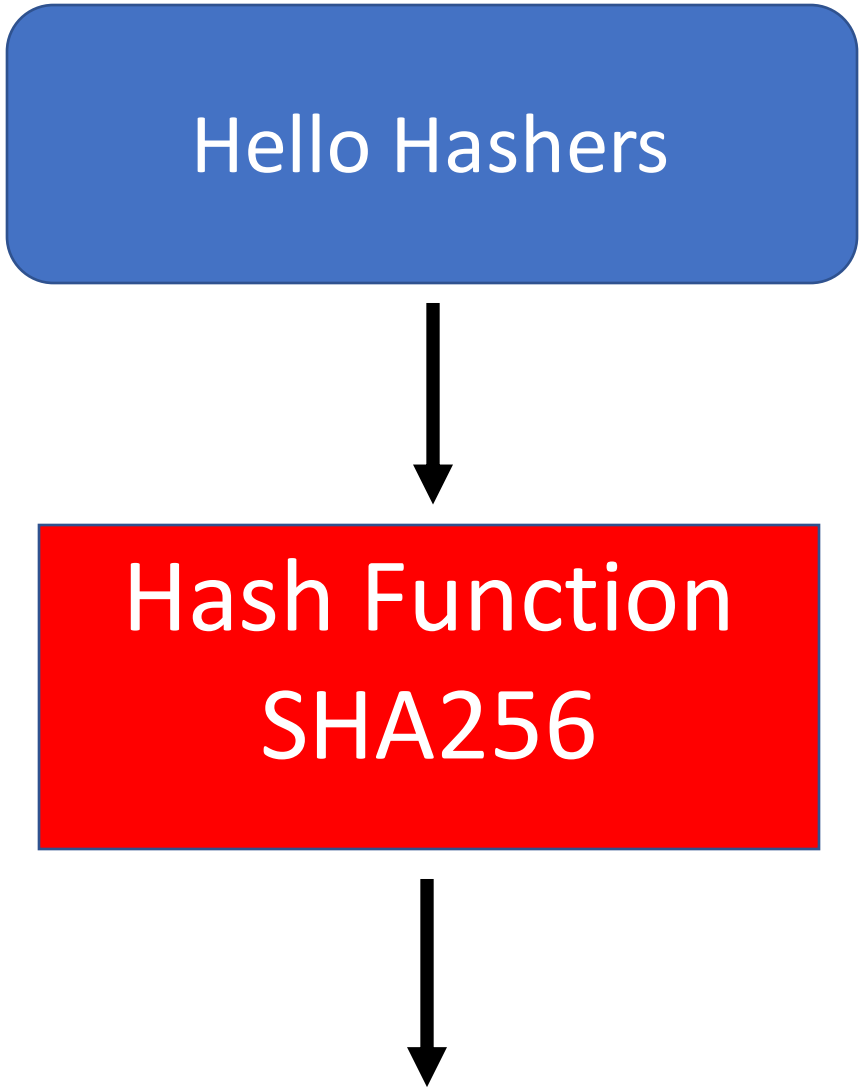
But, in a larger sense, we can not dedicate -- we can not consecrate -- we can not hallow -- this ground. The brave men, living and dead, who struggled here, have consecrated it, far above our poor power to add or detract. The world will little note, nor long remember what we say here, but it can never forget what they did here. It is for us the living, rather, to be dedicated here to the unfinished work which they who fought here have thus far so nobly advanced. It is rather for us to be here dedicated to the great task remaining before us -- that from these honored dead we take increased devotion to that cause for which they gave the last full measure of devotion -- that we here highly resolve that these dead shall not have died in vain -- that this nation, under God, shall have a new birth of freedom -- and that government of the people, by the people, for the people, shall not perish from the earth.

Abraham Lincoln
November 19, 1863

Here is a hash of the Gettysburg Address

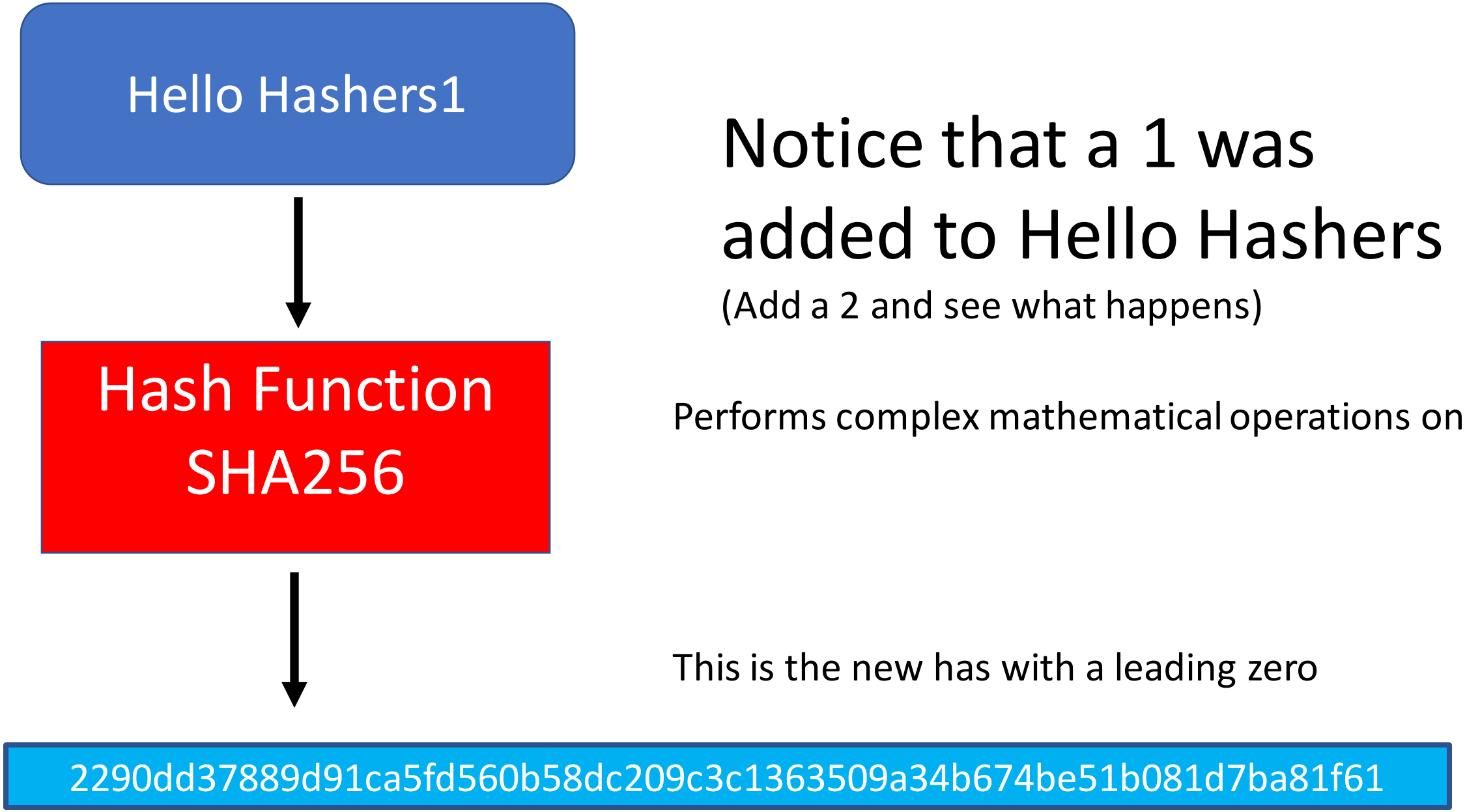
4f23fe7c7432150928278 0d70627bb9b537411855beb823ee52a0cfd7a1c76d9

Hashing Example



Performs complex mathematical operations on text

Data from the hash function is of a fixed size



Notice that a 1 was added to Hello Hashers

(Add a 2 and see what happens)

Performs complex mathematical operations on text

This is the new has with a leading zero

If we just change the *y* to an *i*, we get a different hash value with the SHA 256 program.

Jody 3 BARTS to Sean

03A5F7343B1BD18F72C619092AB7332876CF9DBDC625544391C5B3289628F7C9

Jodi 3 BARTS to Sean

959FC50D00A9FD7AE21E523B228EE030D10AB3F88688F332C0107A2283EA4989

This is how programmers implement a hashing function in php

Hashing this

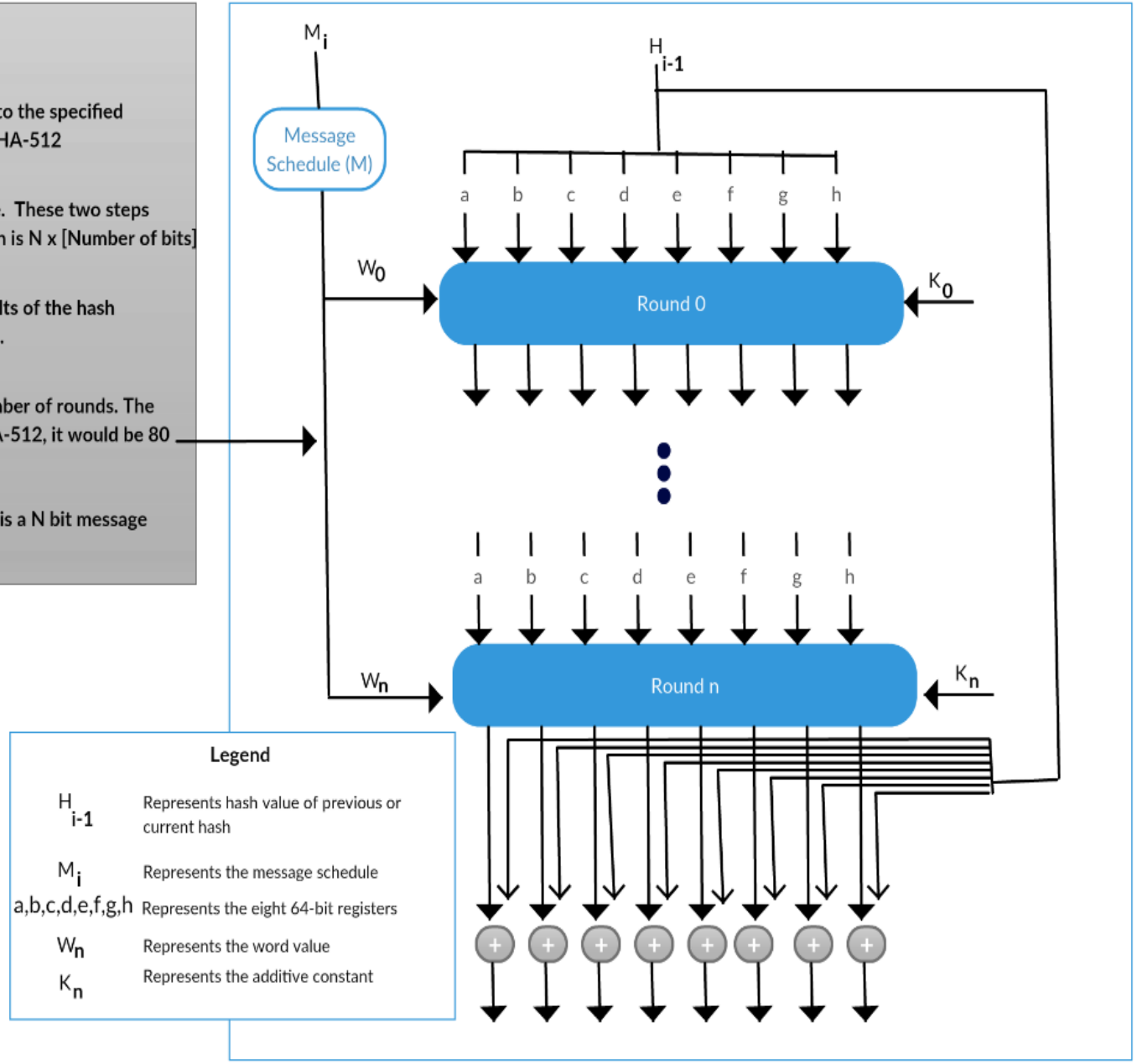
It doesn't matter how large your text is.

Generates this

575d72eae0dcf91376577c54eabaa1eea7c8a61b1874e8ad305c3c84f9148b16

SHA Algorithm Steps

Step 1: Append Padding Bits	The message is padded so that its length is equivalent to the specified number of bits. For example 1 to 1024 in the case of SHA-512
Step 2: Append Length	A specified block of [x] bits is appended to the message. These two steps equate to a total length of the expanded message which is N x [Number of bits]
Step 3: Initialize Hash Buffer	A buffer is used to hold the intermediate and final results of the hash function. In the case of SHA-512, the buffer is 512 bits.
Step 4: Process in 1024-bit (128 byte) blocks	The algorithm step here is to go through a specific number of rounds. The number of rounds is either 64 or 80. In the case of SHA-512, it would be 80 rounds.
Step 5: Output	After all N bit blocks have been processed the output is a N bit message digest.



Technical overview of how SHA Algorithms Work: Don't worry about this!

Adapted and redrawn by Sean Sanders from Cryptography and Network Security Principles and Practice Seventh Edition

Example of PHP call to the hashing algorithm

https://www.w3schools.com/php/phptryit.asp?filename=tryphp_compiler

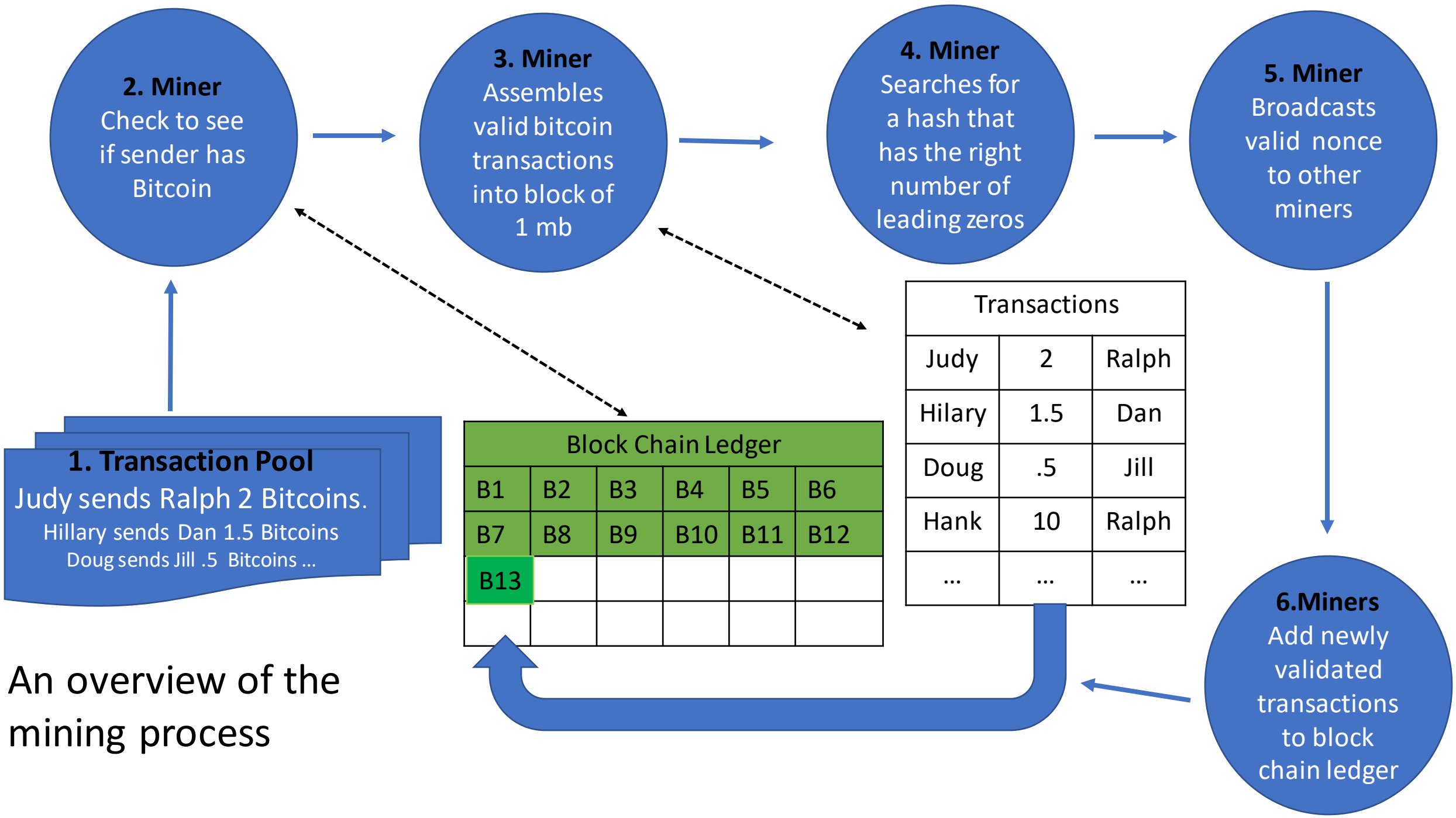
```
<!DOCTYPE html>
<html>
<body>

<?php
$txt = "Hello Hashers";
echo "<b>Input Text:  </b>$txt";
$hash = hash('sha256', $txt);
echo "<br>";
echo "<b>Output:</b> $hash";

?>

</body>
</html>
```

To Summarize



An overview of the mining process

Here is a hash of a block of cryptocurrency transaction pool needing 5 leading zeros

SHA 256 Hash algorithm

Bob sends 5 BARTS to Ann
Jill sends 2 BARTS to Doug
Helen sends 12 BARTS to Julia
Arjen sends13 BARTS to Helen
Joana sends 1 BARTS to Arun
Chul sends 5 BARTS to Ann
Caliope sends 13 BARTS to Lewis
Zinion sends 25 BARTS to Dom
Les sends 5 BARTS to Penney
Goldie sends 8 BARTS to Doug
Vincent sends 5 BARTS to Devanash

000006fffc3f65c8ce411d0392a817b2a767fb4748dd9a7a21f407d673807711

Hash Values for last occurrence is: 000006fffc3f65c8ce411d0392a817b2a767fb4748dd9a7a21f407d673807711
Nonce value is: 102,281,107
Total Number of attempts is: 1,234,179
The Expected number of attempts is: 1,048,576
Start Time is: 0.001 Seconds
End Time is: 7.666 Seconds


BARTS

BARTS Simulation and exercises

- Helps understanding blockchain mining transactions without becoming bogged down in the technical details.
- The BARTS simulation is a non-technical simulation where participants mine or validate a digital coin transaction for buying and selling drawings

Artist draws picture

Artist agrees on BARTS price to buyer

Miners validate BARTS transaction

Validated BARTS transaction added to ledger

Buyer receives drawing from artist

The Blockchain ART Simulation (BARTS)

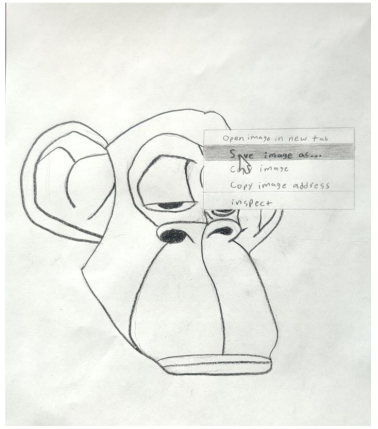
https://artbarts.com/

- The initial coin offering for the 200 million BARTS tokens took place in July of 2018. Two hundred famous pencil artists received 1,000 to 20,000 BARTS tokens if they agreed only to sell their pencil drawings through the ARTBARTS network for three years. Also, over 10,000 gallery owners, investors, dealers, collectors, and even artists purchased 60 million BARTS for approximately $100 million in US funds.
- There are now over 60,000 artists and buyers participating in the marketplace. BARTS miners must use the inter-active online mining software for solving a hash problem.
- You all have BARTS tokens for buying and selling art.
- Here is and example of a BARTS wallet that would be used to buy and sell art online. https://marvelapp.com/prototype/fh036g4

What we need

- Volunteers to draw pictures. Volunteers to purchase the art.
- Draw for 5 minutes. You do not have to be a good artist.
- Then entire class will bid on the art. You all get BARTS. You can keep the BARTS or purchase the art. You can combine your BARTS with others to purchase the art.
- The entire class will add the names of the sellers and buyers to the blockchain. You will all be BARTS miners. If you win the mining competition, you will get a BARTS



Lets *hash* using BARTS mining program

- Go to www.artbarts.com
- Scroll down and click on the following link
- https://tinyurl.com/BARTSMining

- You will start by adding a number to the end of the transaction and then hashing the transaction. This is done repeatedly until you find a hash with one leading zero.

- The first person that finds a hash with one leading zero should yell out Eureka.

Blockchain Ledger Program

This is a program designed to aid in the understanding the addition of transactions to a blockchain ledger.

Only the miners use this program.

Sender Name: Will

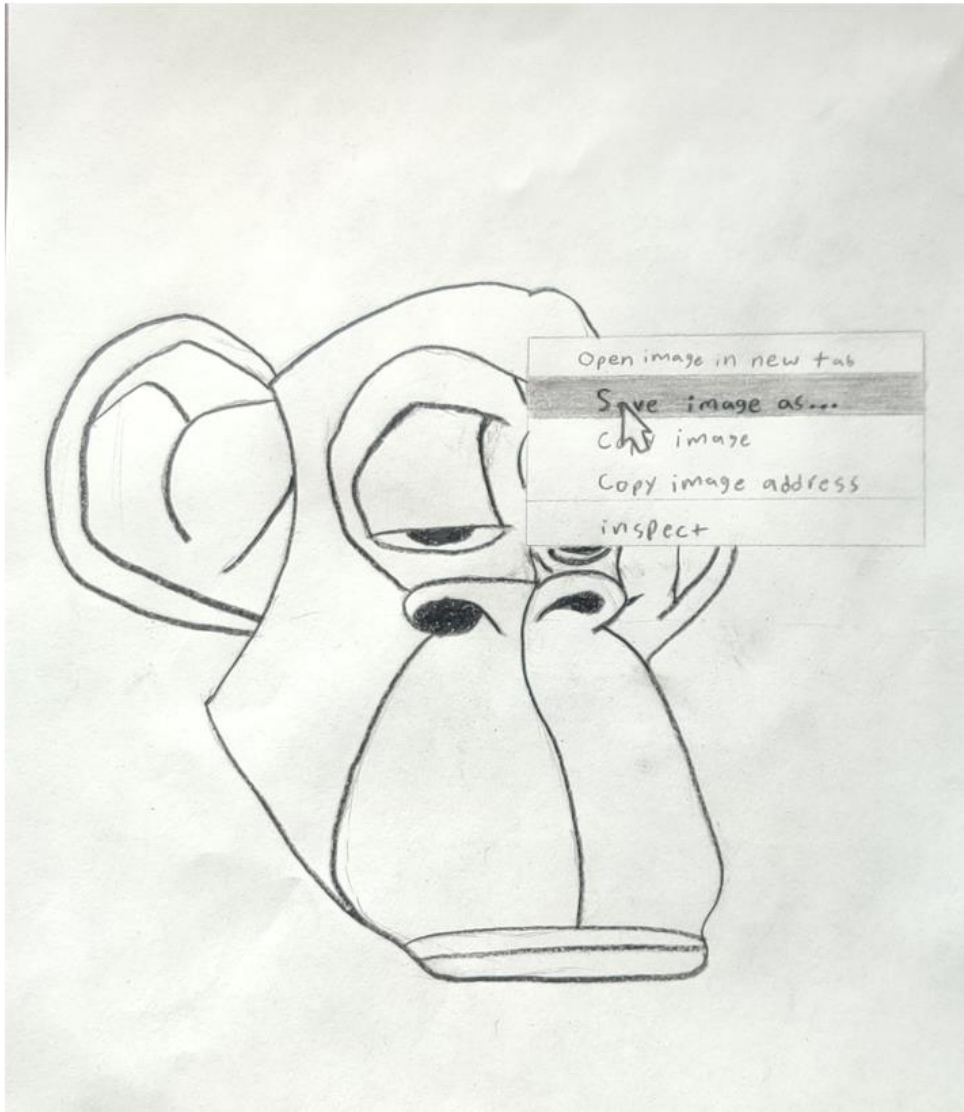
Amount: 1

Receiver Name: Bruce

Nonce: 1

Submit

Hash Value: 314019d8b0812ed64130cdad9e2b0eefb026caa2756ba3eeab6efc69da1a7d5b



How the Nonce is Used in Mining

- In Bitcoin mining the SHA256 hash is generated by adding a nonce or unique value to the end of the text that is being hashed.
- The goal is to generate a SHA256 hash that starts with zeros.
- The nonce is the random number that is added to the end of the text being hashed until the desired number of leading zeros are generated.
- This adding of a random number, or nonce, to generate a hash with leading zeros is what mining is all about.

Let the bidding on the drawings begin.

Here are some drawings from 9/28/2022

Enter in Sender Name: ?

Enter in Amount: 1

Enter in Receiver Name: Ruchika

Enter in Nonce Value: 1

Submit

Created by Ruchika Gehlot
Purchased by ?

Portfolio of 4 Drawings by Sayalee Ramesh Lanjewar
(Bid on all 4)

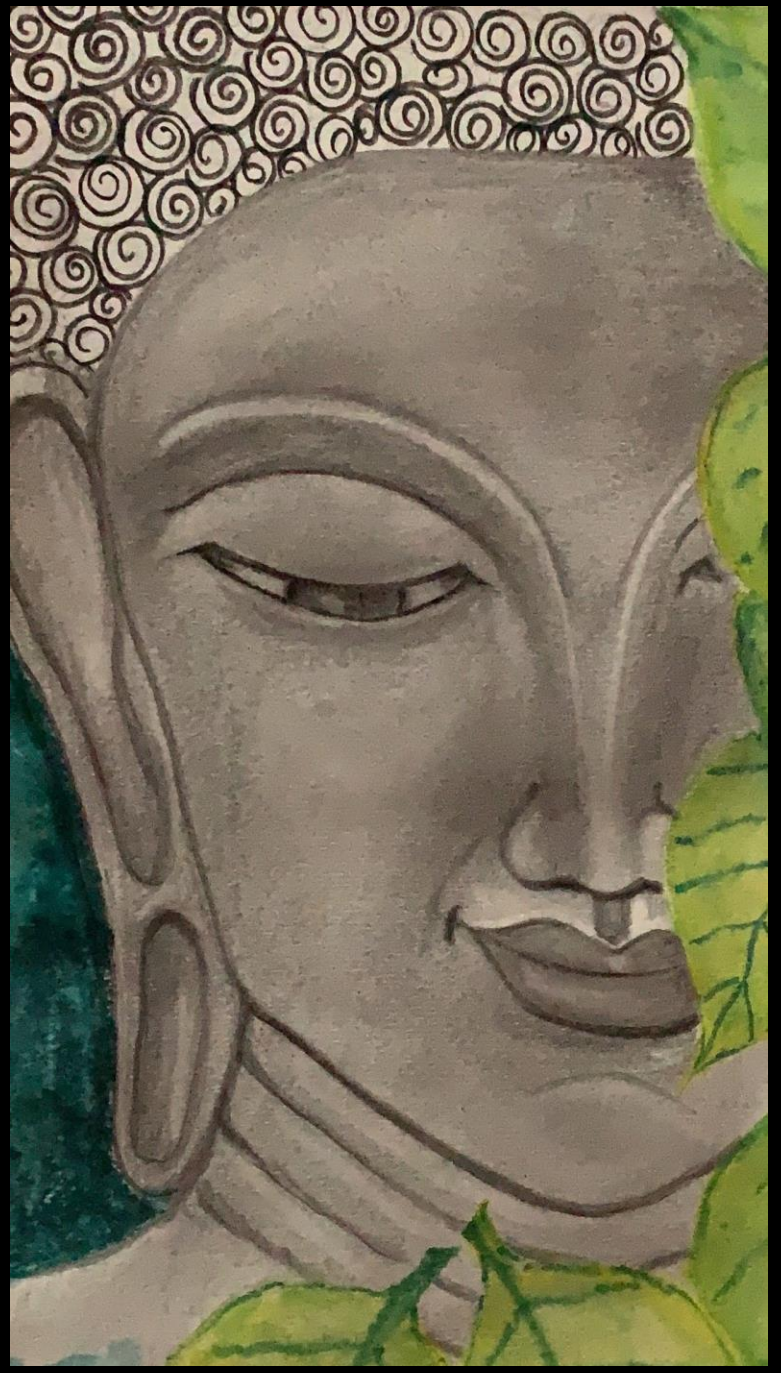
Enter in Sender Name: ?

Enter in Amount: 1

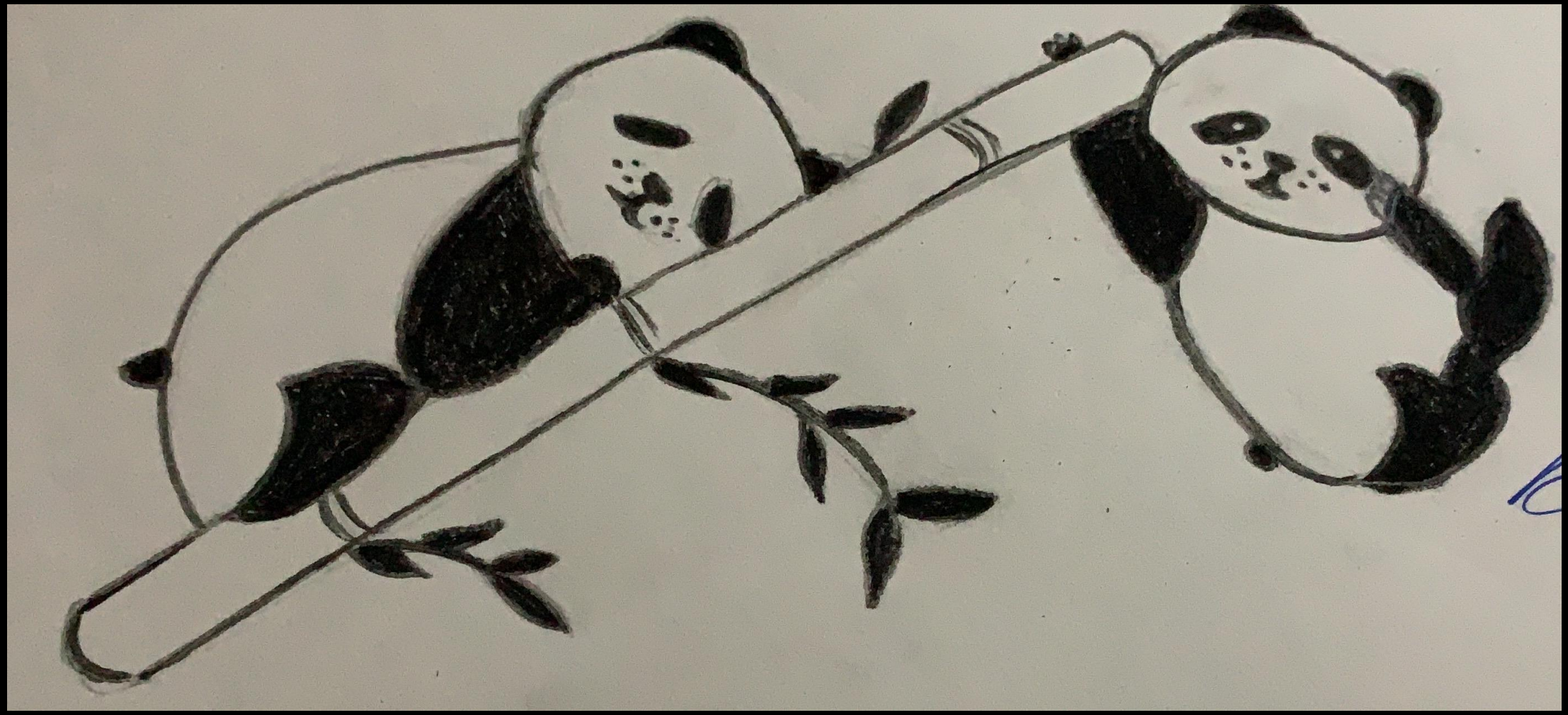
Enter in Receiver Name: Sayalee

Enter in Nonce Value: 1

Submit



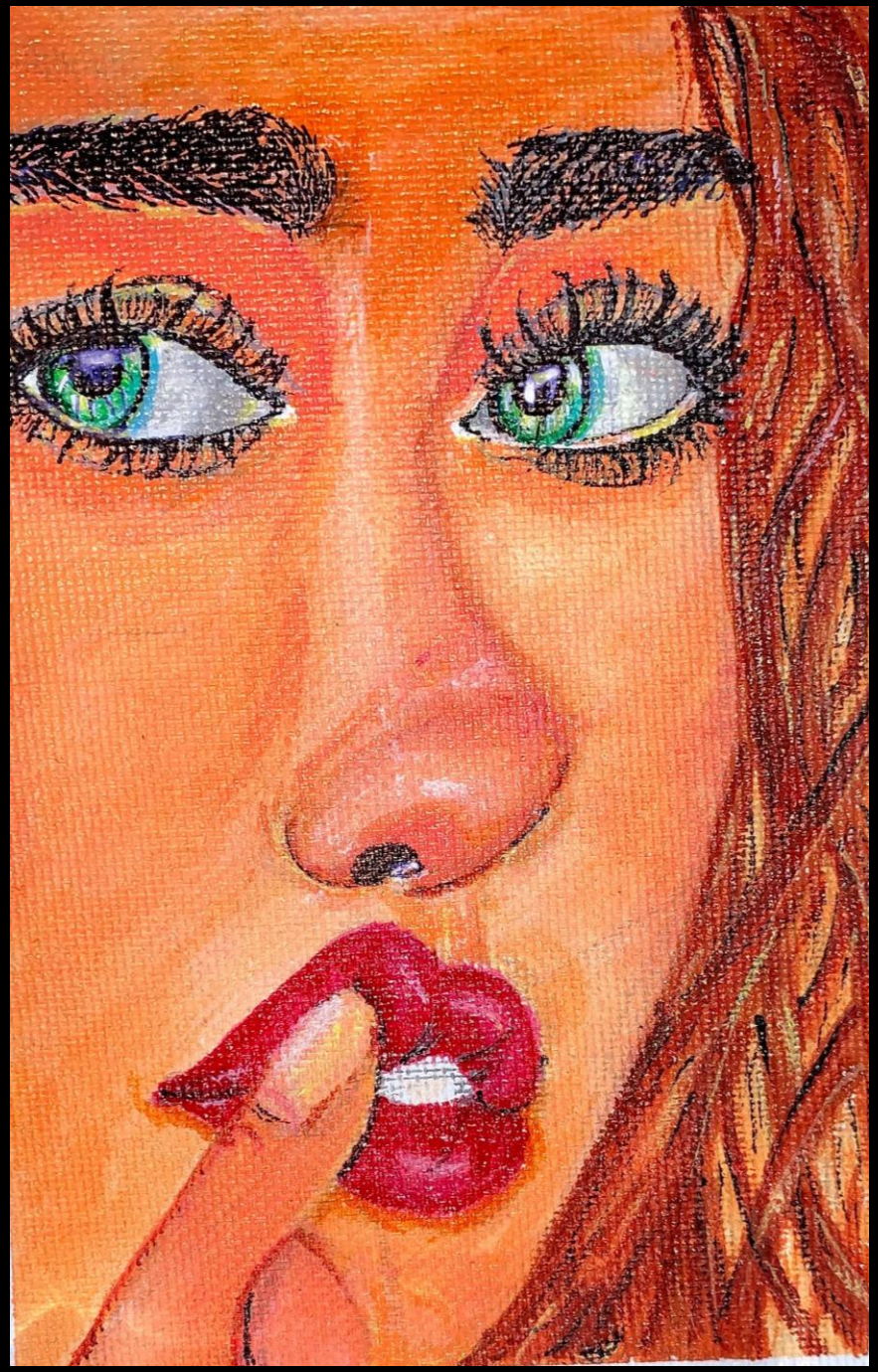
Created by Sayalee Ramesh Lanjewar
Purchased by ?



Portfolio by Sayalee Ramesh Lanjewar

Portfolio by Sayalee Ramesh Lanjewar

Portfolio by Sayalee Ramesh Lanjewar



Enter in Sender Name: ?

Enter in Amount: 1

Enter in Receiver Name: Pooja

Enter in Nonce Value: 1

Submit

Created by Pooja Nirvutti Yede
Purchased by ?

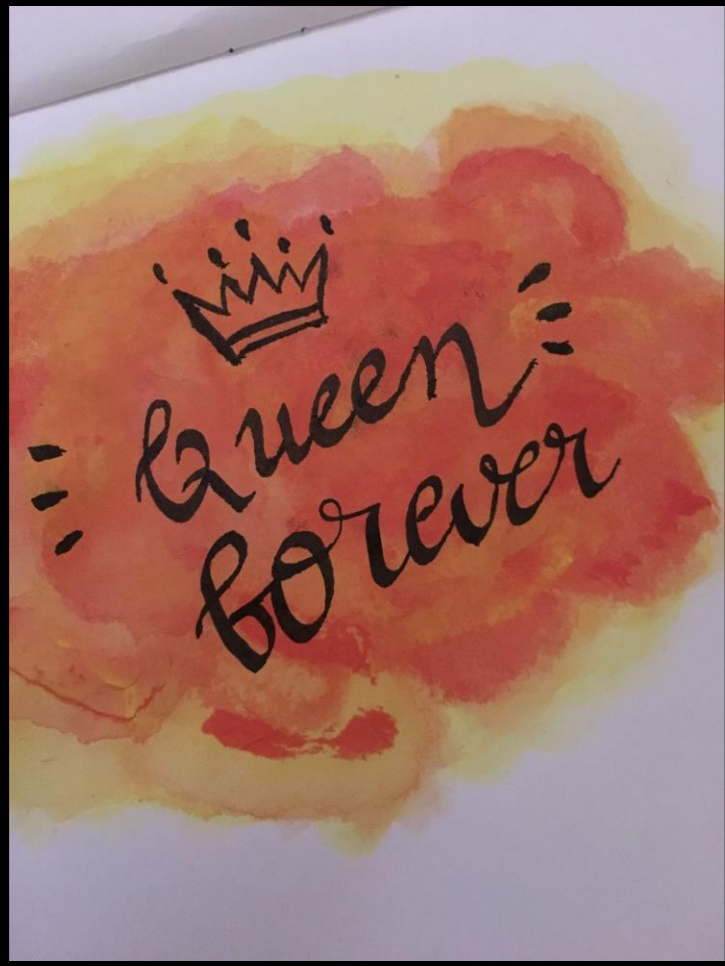
Enter in Sender Name: ?

Enter in Amount: 1

Enter in Receiver Name: Swetha

Enter in Nonce Value: 1

Submit



Created by Swetha Palempalli

Purchased by ?

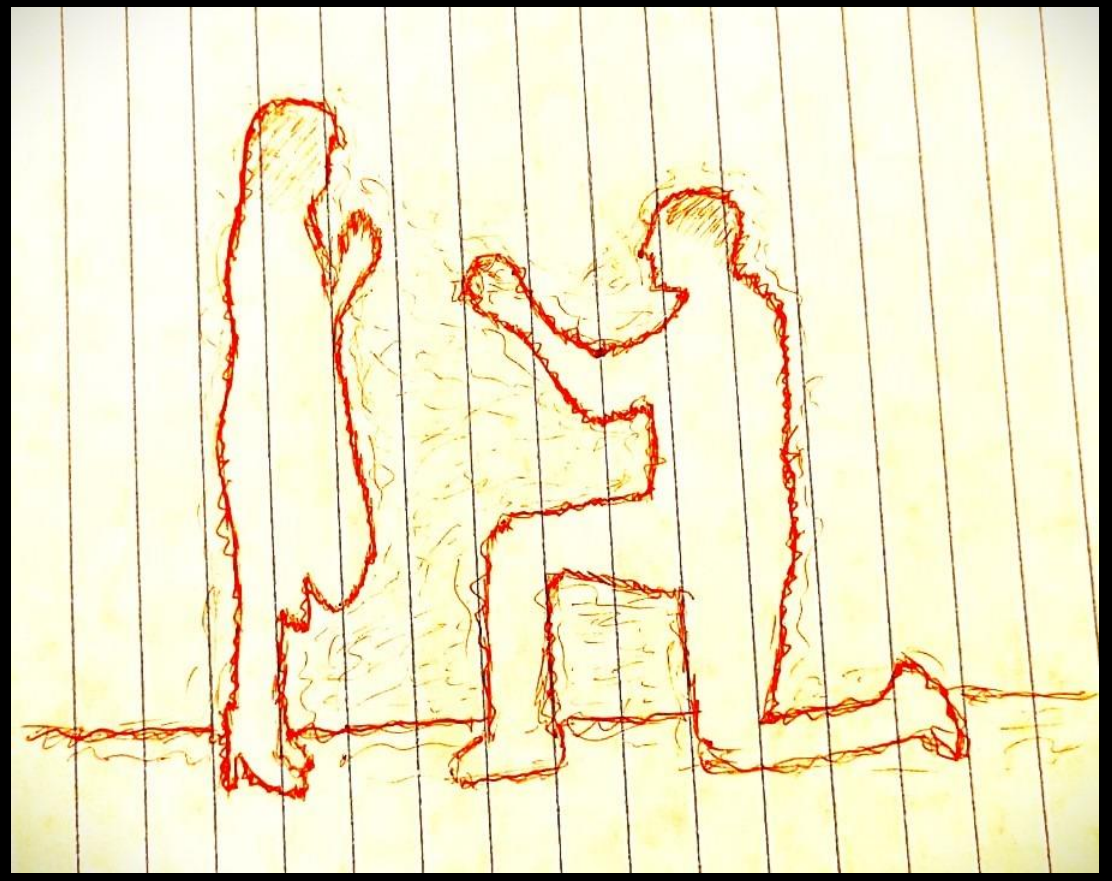
Enter in Sender Name: ?

Enter in Amount: 1

Enter in Receiver Name: Mandeep

Enter in Nonce Value: 1

Submit



Created by Mandeep Vratesh
Purchased by ?

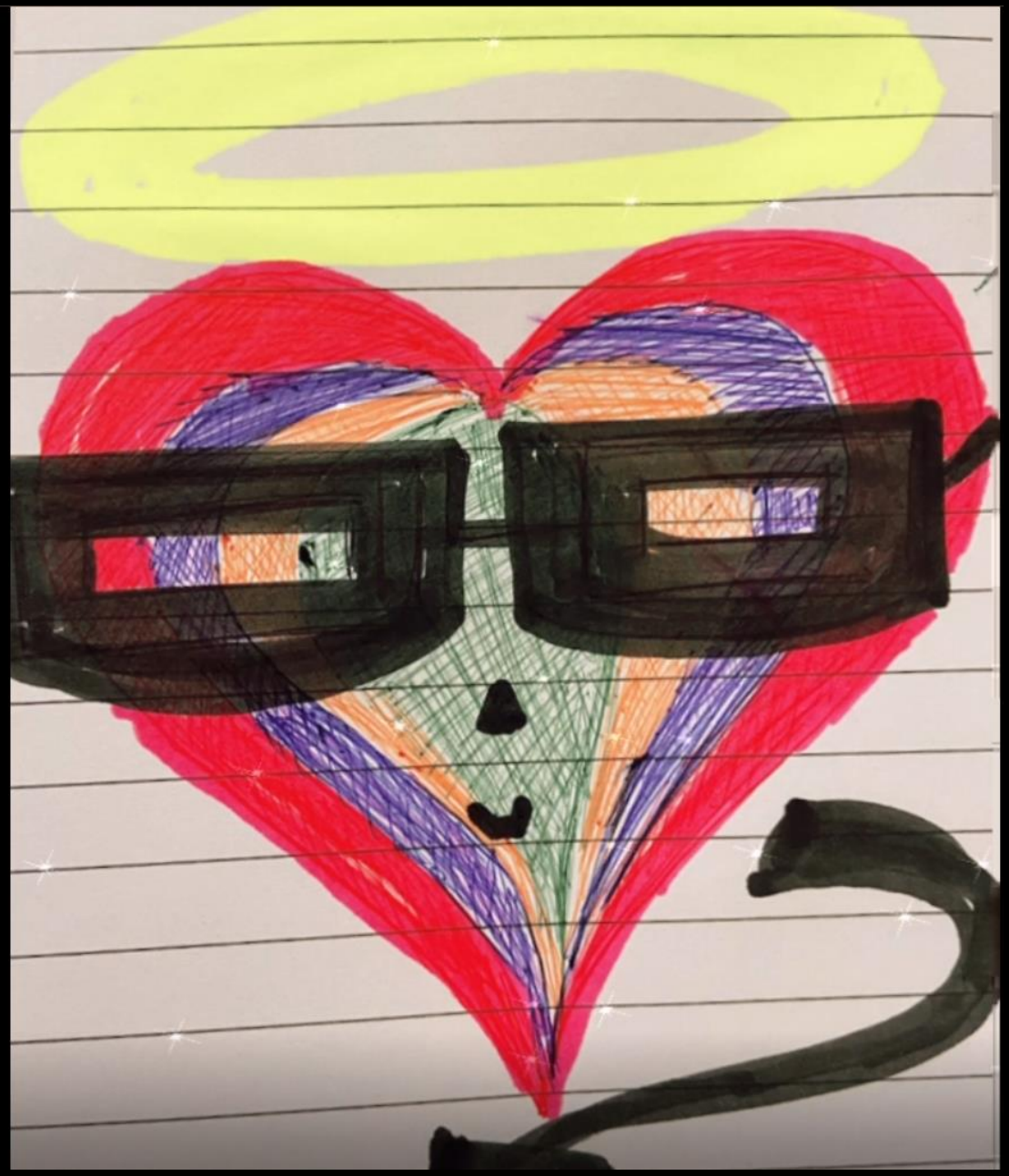
Enter in Sender Name: ?

Enter in Amount: 1

Enter in Receiver Name: Anmol

Enter in Nonce Value: 1

Submit



Created by Anmol Dhawan
Purchased by ?

Enter in Sender Name: ?

Enter in Amount: 1

Enter in Receiver Name: Steven

Enter in Nonce Value: 1

Submit

Created by Steven Arias
Purchased by ?

Enter in Sender Name: ?

Enter in Amount: 1

Enter in Receiver Name: Ayushi

Enter in Nonce Value: 1

Submit

Created by Ayushi
Purchased by ?

Enter in Sender Name: ?

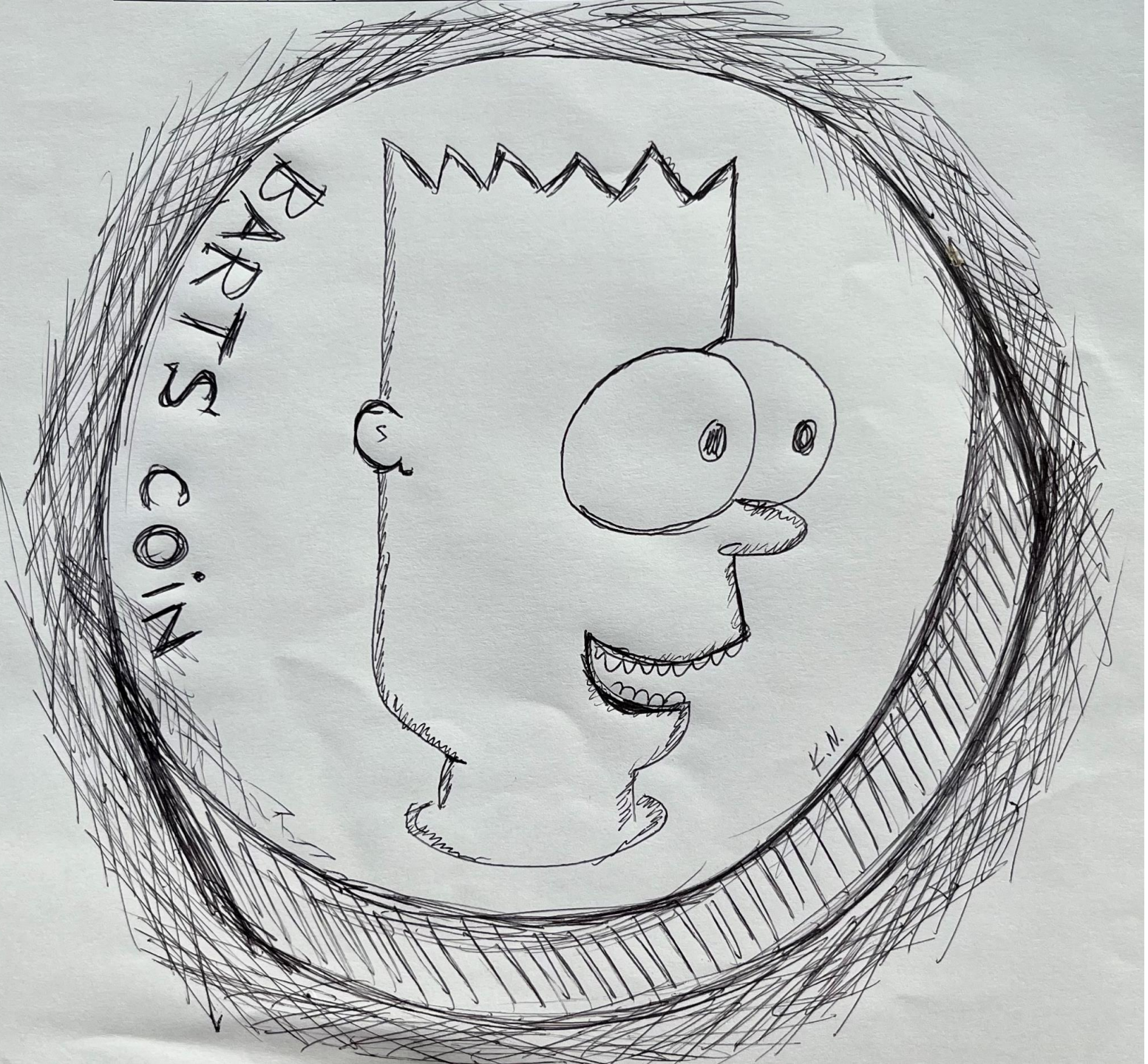
Enter in Amount: 1

Enter in Receiver Name: Sachita

Enter in Nonce Value: 1

Submit

Created by Sachita Shetty
Purchased by ?



Drawn by Krisjanis Nesenbergsis

Now lets modify using Deep Dream Generator

https://deepdreamgenerator.com/

https://www.unite.ai/10-best-ai-art-generators/#:~:text=Another%20one%20of%20the%20best,trained%20with%20millions%20of%20images.


WWW.EARTH.SU

Debriefing

Lets go over additional details

This is a simulation:
Many similarities and several differences.

- Bitcoin blocks usually contains 1,000 to 3,000 transactions.
- Miners also receive transaction fees for Bitcoin.
- The instructor is a centralized validator of the transactions and the participants. Digital currencies use many nodes in a peer-to-peer network to verify transactions.

Oreilly: Mastering Bitcoin

- The blockchain data structure is an ordered, back-linked list of blocks of transactions. The blockchain can be stored as a flat file, or in a simple database. The Bitcoin Core client stores the blockchain metadata using Google's LevelDB database. Blocks are linked "back," each referring to the previous block in the chain. The blockchain is often visualized as a vertical stack, with blocks layered on top of each other and the first block serving as the foundation of the stack. The visualization of blocks stacked on top of each other results in the use of terms such as "height" to refer to the distance from the first block, and "top" or "tip" to refer to the most recently added block.

- Each block within the blockchain is identified by a hash, generated using the SHA256 cryptographic hash algorithm on the header of the block. Each block also references a previous block, known as the parent block, through the "previous block hash" field in the block header. In other words, each block contains the hash of its parent inside its own header. The sequence of hashes linking each block to its parent creates a chain going back all the way to the first block ever created, known as the genesis block.
- https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html

Mempool

- Bitcoin transactions are initially validated by checking the so-called UTXO. This is the Unspent Transaction Output ledger.
- If a Bitcoin sender has the required amount of Bitcoin available to send then it is a valid transaction that can be added to the mempool for final processing.
- Bitcoin valid transactions enter the blockchain for processing (mined) after leaving the mempool waiting room.
- https://medium.com/bitbees/what-the-heck-is-utxo-ca68f2651819

10 Best ASIC Miners For Mining Cryptocurrency In 2022

Last Updated:June 22, 2022

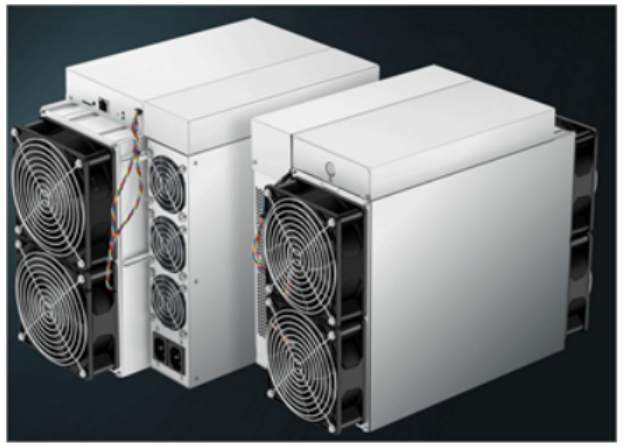
Comparison of the Best ASIC Miners

Name	Weight	Hash rate	Price	Our rating
Antminer S19 Pro	15,500 g	110 Th/s	$2,860	5/5
Minedollars	N/A	Varies per contract	$10 at the minimum	5/5
WhatsMiner M30S++	10,500 g	112TH/s±5%	$3,999	5/5
AVALONminer 1246	12,800 g	90Th/s	$3,890	4.8/5
WhatsMiner M32	10,500 g	68TH/s +/- 5	$3,557	4.5/5
AvalonMiner 1166 Pro	12,800 g	81TH/s	$3,000	4.5/5

Top ASIC Cryptocurrency Miners review:

#1) Antminer S19 Pro

Antminer S19 Pro – Best for most profitable ASIC mining of Bitcoin, Bitcoin Cash, and other SHA-256 algorithm cryptocurrencies.



Public and Private Keys

- You need a **private key** to both send and receive Bitcoin. The private key is necessary to unlock the Bitcoin you receive and send. The private key is in your Bitcoin wallet.
- You send Bitcoin to a **public key**.
- The **public key** is always paired with a unique **private key**
- The steps for receiving a transaction.
- Go here for an overview of sending Bitcoin.
  - https://www.gemini.com/cryptopedia/send-and-receive-crypto-bitcoin-transfer

Mining Difficulty is controlled by the number of leading zeros required

- The goal of the Bitcoin mining infrastructure is to mine a block in about 10 minutes.
- If the total hashing mining power increases, then the number of zeros required increases. If the total hashing power for all of the miners decreases then the number of zeros required decreases.

- Hash with 1 zero requires about 16^{1} or 16 attempts.
- Hash with 2 zeros requires about 16^{2} or 256 attempts.
- Hash with 3 zeros requires about 16^{3} or 4,096 attempts.
- Hash with 4 zeros requires about 16^{4} or 65,536 attempts.
- Hash with 5 zeros requires about 16^{5} or 1,048576 attempts.
- Hash with 19 zeros requires about 16^{19} or

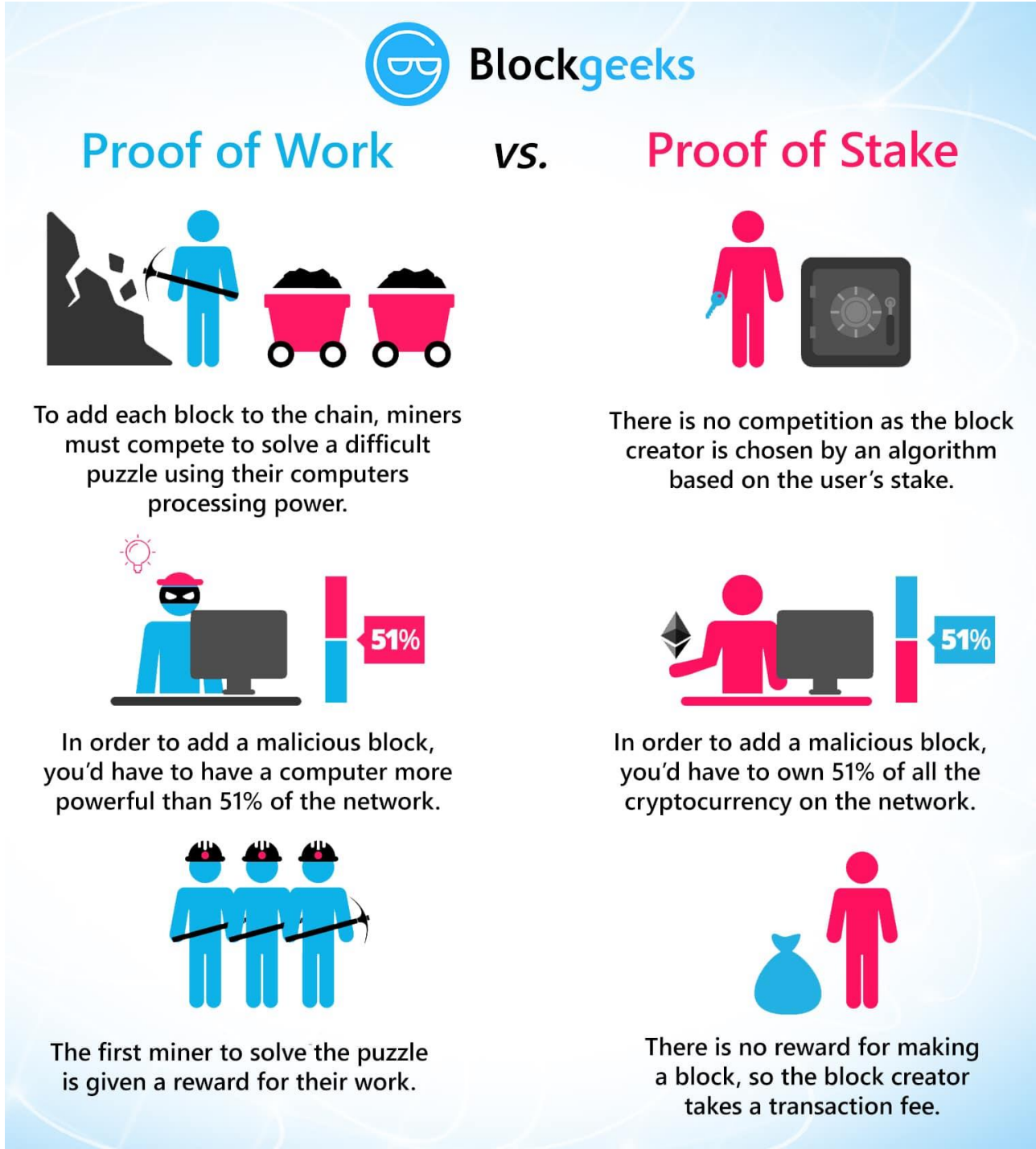
  75,557,863,725,914,323,419,136 attempts.

Consensus approaches for miners differ by platform

- Achieving **consensus** in Bitcoin mining involves verifying that the Bitcoin transactions in a block reflect truth. That is the senders have the Bitcoin and have not spent it before and that everyone has a valid account. Here is an interesting, technical, and free chapter on mining consensus.
- **Proof of work** (Bitcoin and BARTS): Miners try to solve hash problem. The first miner to solve the hash problem will get a reward, (now only 6.25 Bitcoins) the hash transaction will be added to the blockchain after it has been validated by other miners.
- **Proof of stake** (Ethereum?): One miner or validator is randomly selected to mint new blocks. The minter node with the highest number of coins in possession has a higher probability of being elected as the forger for the new block.

Current News

https://www.reddit.com/r/CryptoCurrency/



Typical Block Statistics for Mining

On March 02, 2022 there were around one million Bitcoin miners performing **195 million trillion** hashes over a 24 hour period to find a hash for Block 725630 with 19 zeros. Here are the block statistics

Block 725630

This block was mined on March 02, 2022 at 2:43 PM EST by AntPool. It currently has 1 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC ($273,562.69). The reward consisted of a base reward of 6.25000000 BTC ($273,562.69) with an additional 0.12518932 BTC ($5,479.54) reward paid as fees of the 2773 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 4,755.18497759 BTC ($208,134,589.12) were sent in the block with the average transaction being 1.71481608 BTC ($75,057.55).

Hash 00000000000000000405ce371d1132e226335a0d3f8314a43a5c37cb2a5485

Why the biggest Bitcoin Mines are in China: https://spectrum.ieee.org/bitcoin-mining

Block Stat for October 19, **Block 759,412**

Bitcoin Block #759,412

Mined on 10/19/2022, 14:40:18 View all Blocks

This block was mined on 10/19/2022, 14:40:18 by Binance Pool. A total of 24,011.09 BTC ($460,613,058) were sent in the block with the transaction being 6.3893 BTC ($122,568). Binance Pool earned a total reward of 6.25 BTC $119,895. The reward consisted of a base re 6.25 BTC $119,895 with an additional 0.3381 BTC ($6,485.89) reward paid as fees of the 3,758 transactions which were included in the

Details

Hash	00000-27913	Size	1,420,370
Depth	1	Version	0×20000000
Capacity	135.46%	Merkle Root	69-dc
Distance	19m 5s	Difficulty	35,610,794,164,371.65
BTC	24,011.0856	Nonce	553,525,204
Value	$460,613,058	Bits	386,393,970
Value Today	$460,709,342	Weight	3,993,179 WU
Average Value	6.3893255896 BTC	Median Time	Oct 19, 2022, 2:17:35 PM
Median Value	0.02585435 BTC	Minted	6.25 BTC
Input Value	24,011.42 BTC	Reward	6.58806779 BTC
Output Value	24,017.67 BTC	Mined on	Oct 19, 2022, 2:40:18 PM
Transactions	3,758	Height	759,412
Witness Tx's	3,207	Confirmations	1
Inputs	5,710	Miner	Binance Pool

Some Bitcoin Stats and Places

- Current Price: https://www.coindesk.com/price/bitcoin
- Blockchain charts: https://www.blockchain.com/charts
- Block explorer: https://www.blockchain.com/btc/blocks
- Where to complain if you are rekt: https://www.reddit.com/r/CryptoCurrency/
- Initial Coin Offerings News: https://cointelegraph.com/tags/ico
- BITMAIN Antminer: https://www.bitmain.com/

Some Terms of the Trade

- Altcoin: An altcoin is a digital currency other than bitcoin.
- FOMO: The term "FOMO" stands for the phrase "fear of missing out.“
- HODL: Sort of stands for "hold on for dear life.
- FUD: Fear, uncertainty and doubt.
- Initial Coin Offering (ICO): offering digital tokens to the public in an effort to raise money
- Moon/Mooning: means digital currency rises sharply in value.
- Pump and Dump: Market participants work together to inflate the price currency then sell it when its value is artificially high.
- Rekt: Crypto trader has lost substantial amounts of money
- Whale: The term used to describe a trader who makes large crypto trades.

The following slides show more student drawings

https://flic.kr/s/aHsmVGJsuP

Enter in Sender Name: Bruce

Enter in Amount: 5

Enter in Receiver Name: Samantha

Enter in Nonce Value: 1

Submit

Created by Samantha Weinberg
Purchased by Bruce Hepel

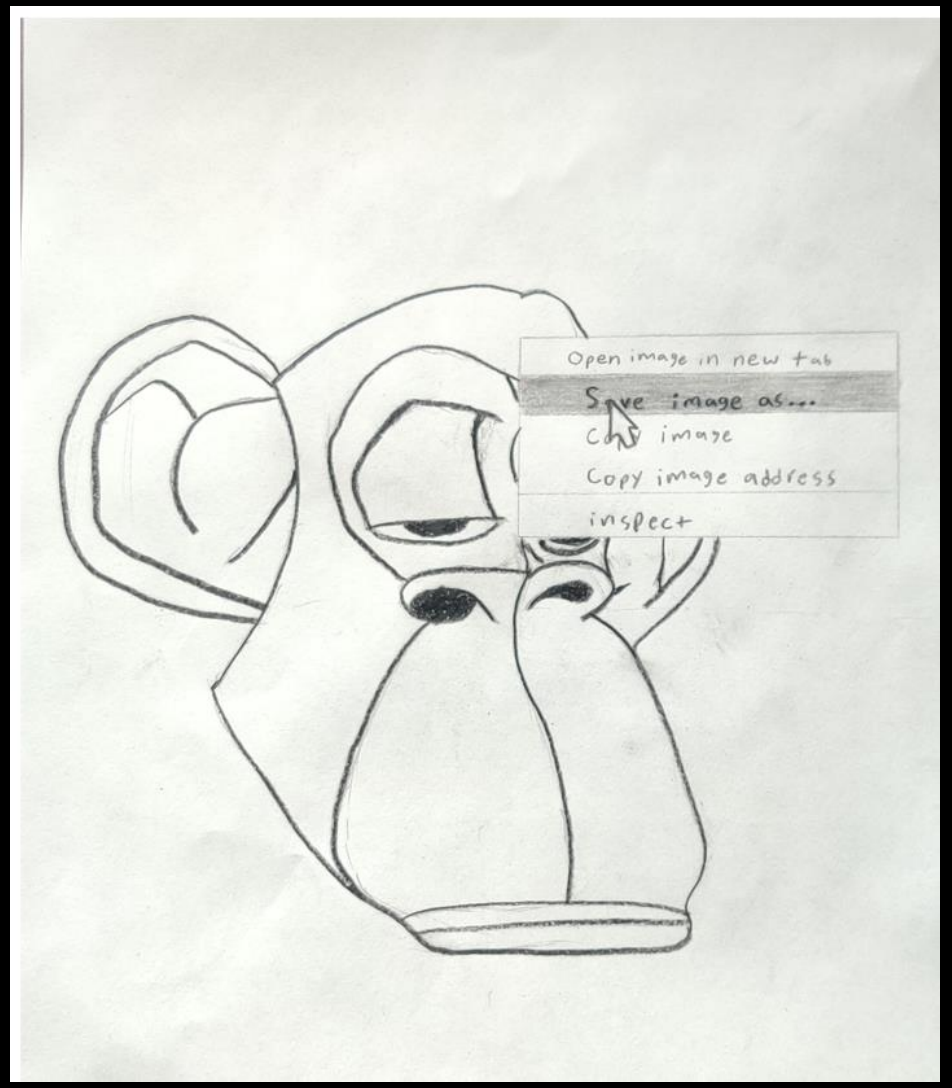
Enter in Sender Name: Will

Enter in Amount: 1

Enter in Receiver Name: Bruce

Enter in Nonce Value: 1

Submit



Created by Bruce Hepel
Purchased by Will Peterson

Enter in Sender Name: Christopher

Enter in Amount: 20

Enter in Receiver Name: Christopher

Enter in Nonce Value: 1

Submit

Created by Christopher Munoz Guzman
Purchased by Christopher Munoz Guzman

Enter in Sender Name: Joseph

Enter in Amount: 10

Enter in Receiver Name: Zhiqi

Enter in Nonce Value: 1

Submit

Created by Zhiqi Jiang
Purchased by Joseph Contrino

Enter in Sender Name: Tatjana

Enter in Amount: 10

Enter in Receiver Name: Othniel

Enter in Nonce Value: 1

Submit

Created by Othniel Lambert
Purchased by Tatjana Tamborvceva

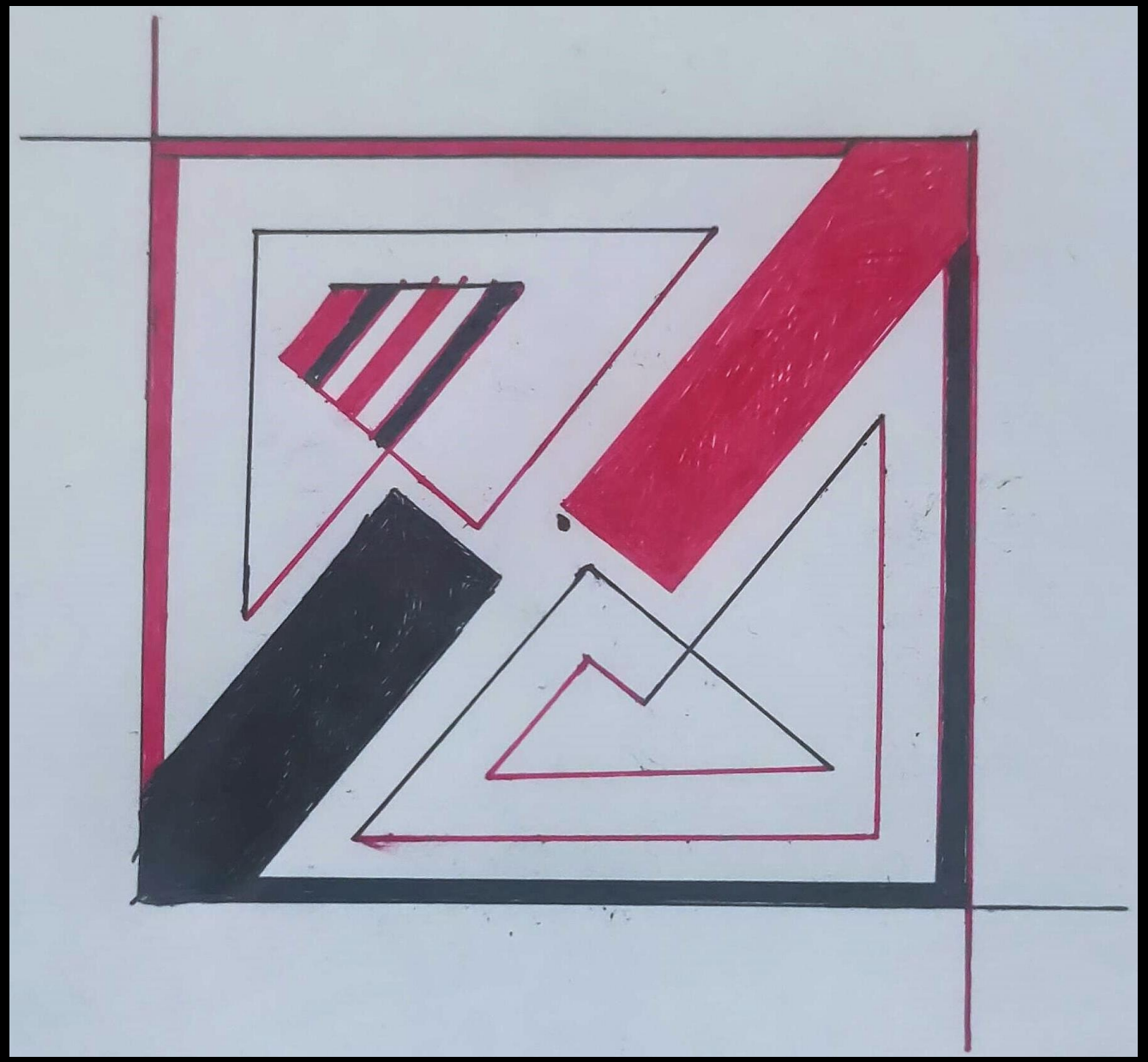
Enter in Sender Name: Michael

Enter in Amount: 10

Enter in Receiver Name: Akash

Enter in Nonce Value: 1

Submit



Created by Akash Garg
Purchased by Michael Taylor

Enter in Sender Name: Elina

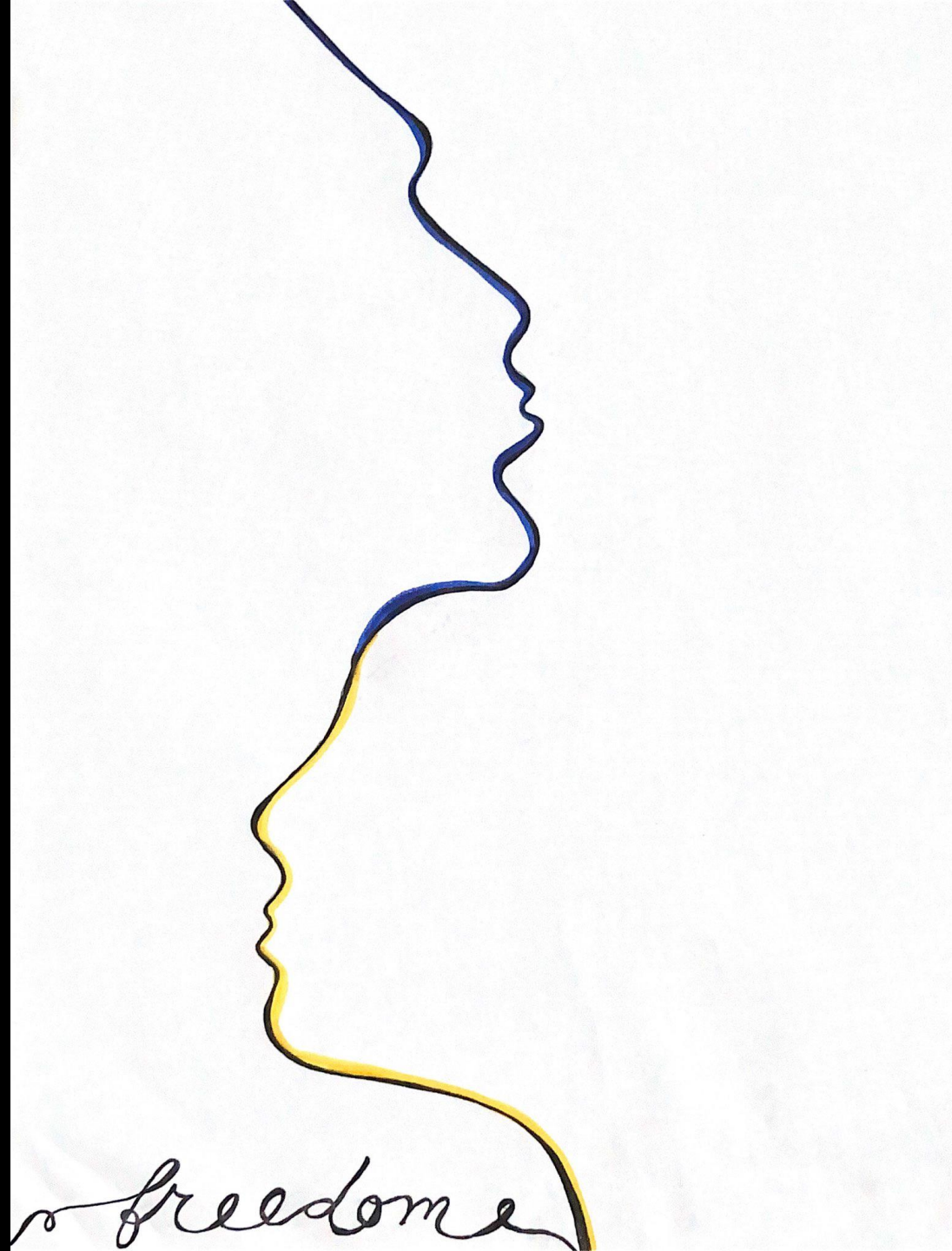
Enter in Amount: 20

Enter in Receiver Name: Anu

Enter in Nonce Value: 1

Submit

Created by Anu Patel
Purchased by Elina Lidere



Enter in Sender Name: Neeraj

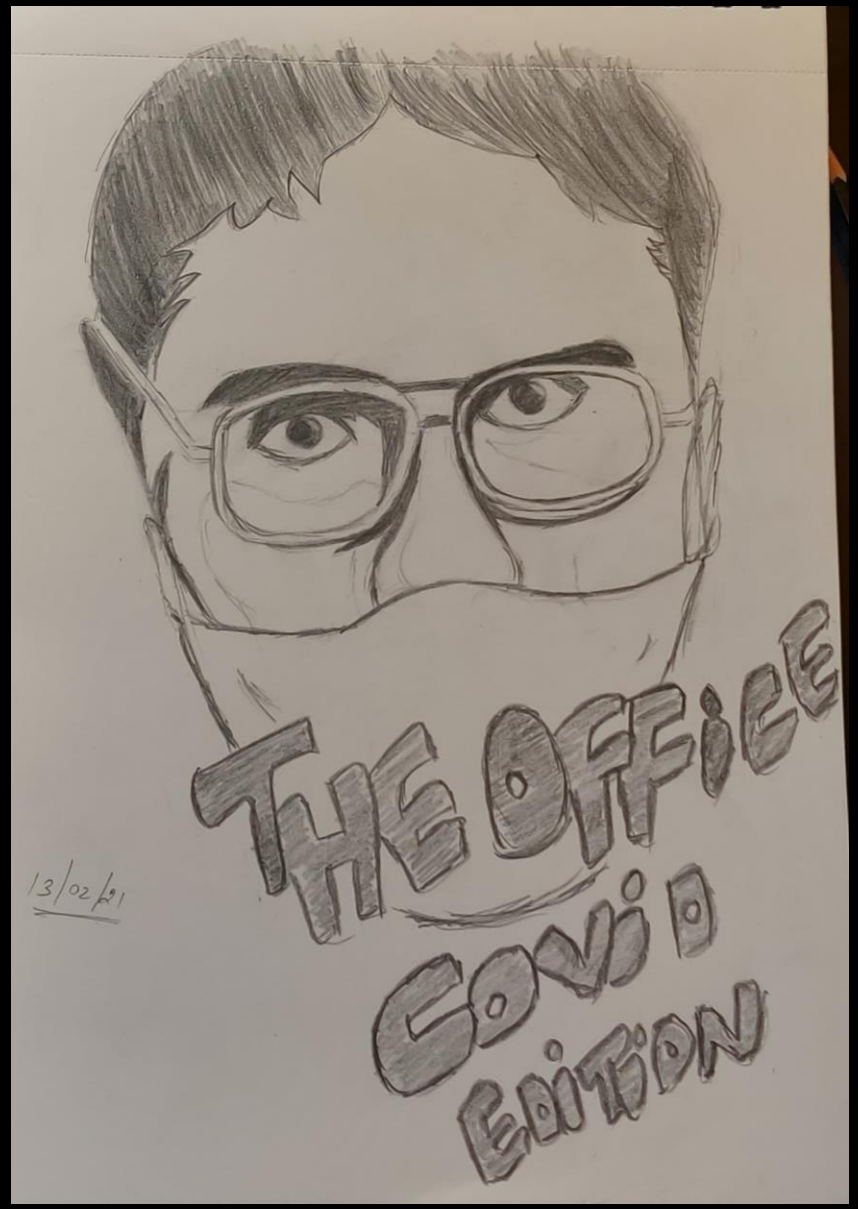
Enter in Amount: 10

Enter in Receiver Name: Janki

Enter in Nonce Value: 1

Submit

Created by Janki
Purchased by Neeraj



Enter in Sender Name: Nandita

Enter in Amount: 12

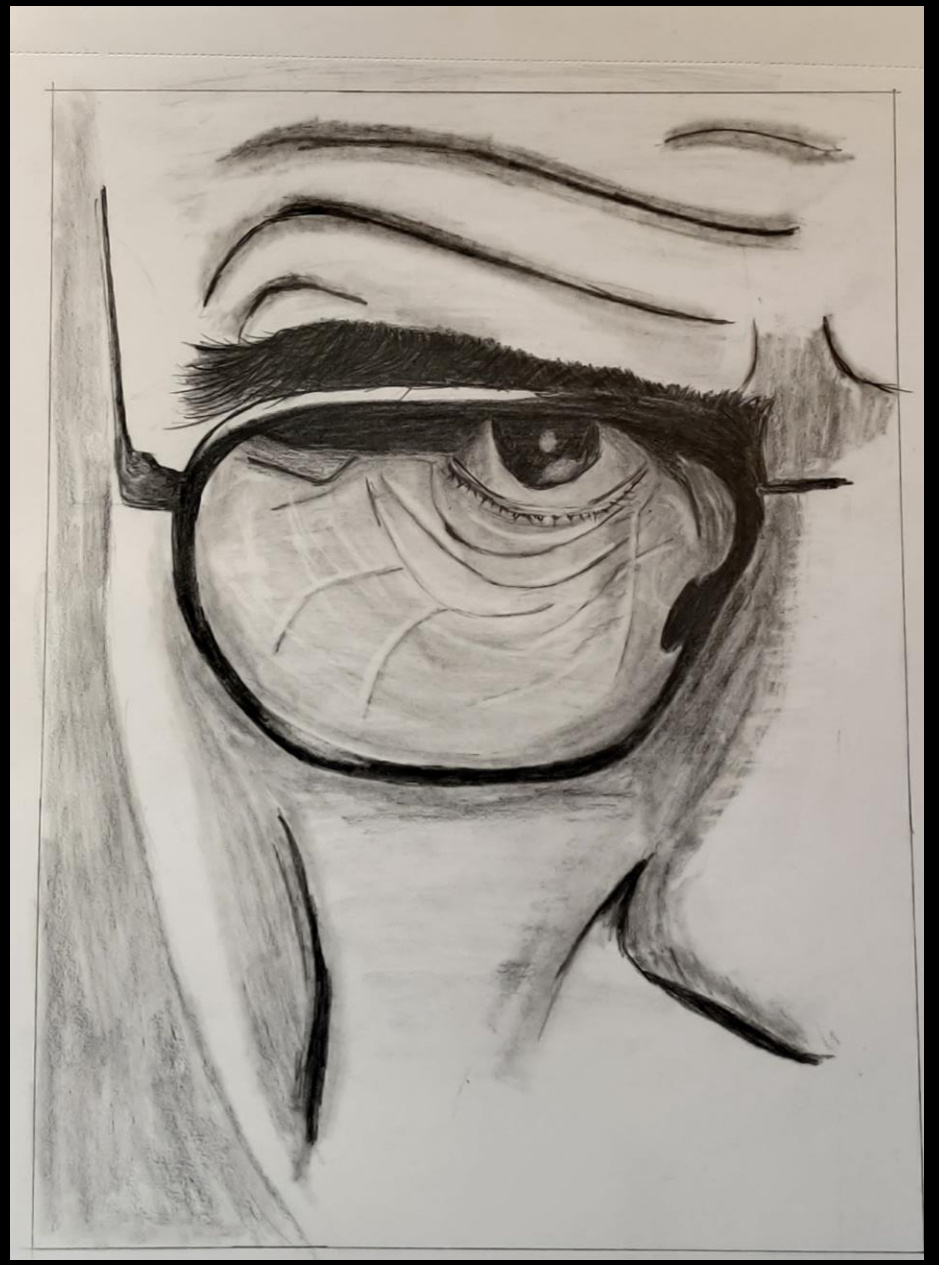
Enter in Receiver Name: Janki

Enter in Nonce Value: 1

Submit

Created by Janki
Purchased by Nandita

Walter White – Breaking Bad



Enter in Sender Name: Nandita

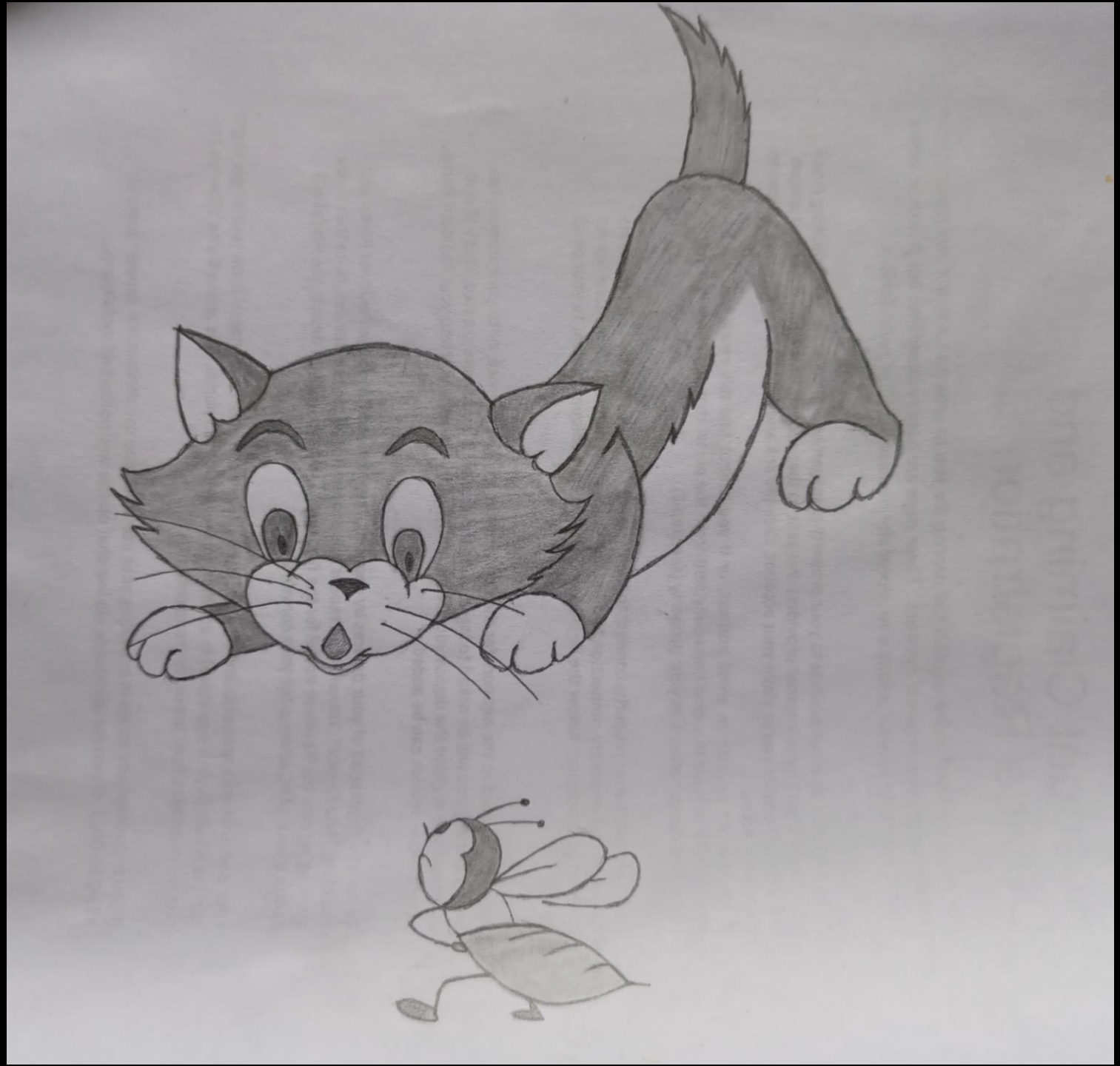
Enter in Amount: 8

Enter in Receiver Name: Chethana

Enter in Nonce Value: 1

Submit

Created by Chethana
Purchased by Nandita



Enter in Sender Name: Saurav

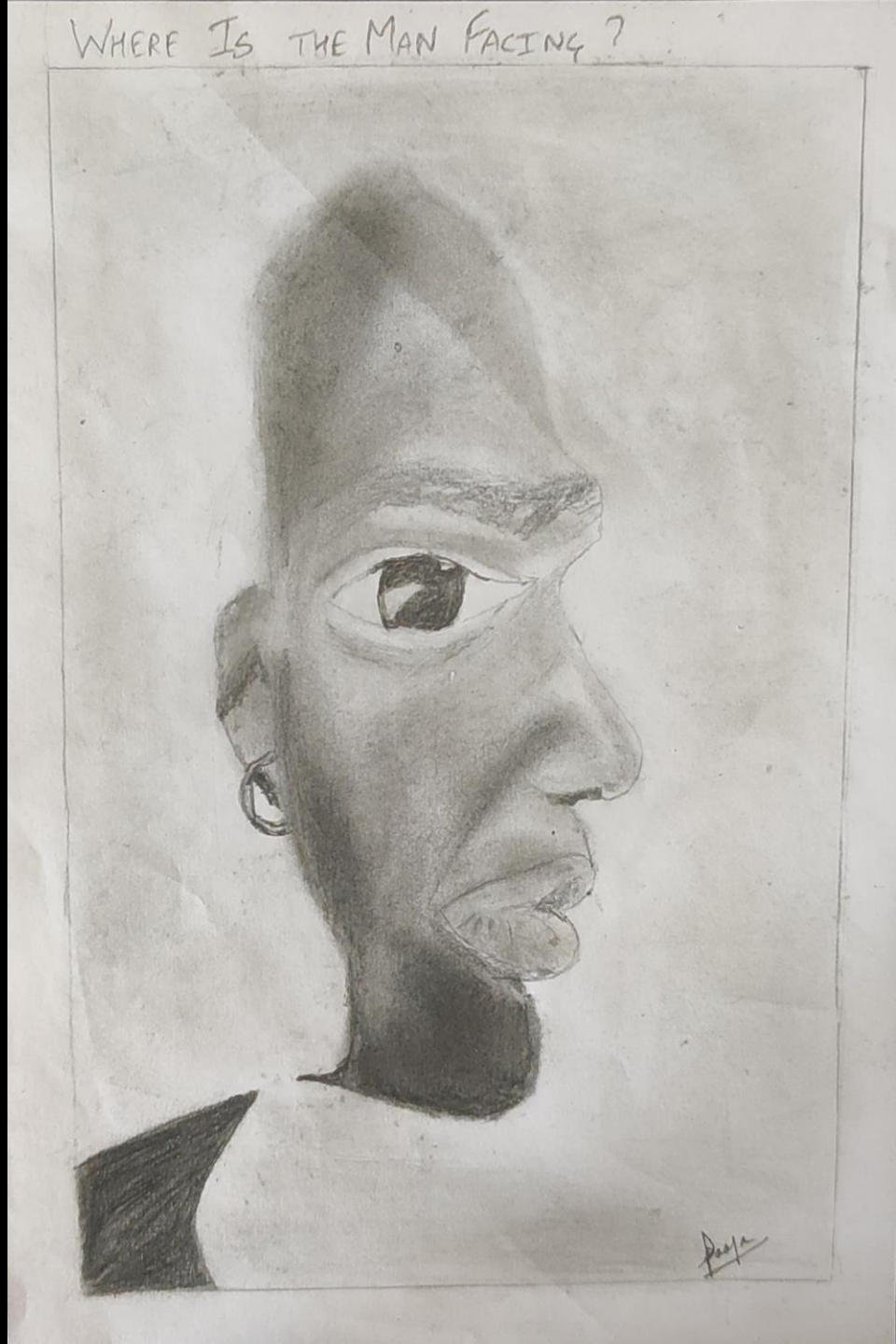
Enter in Amount: 15

Enter in Receiver Name: Pooja

Enter in Nonce Value: 1

Submit

Created by Pooja
Purchased by Saurav



Enter in Sender Name: Utsav

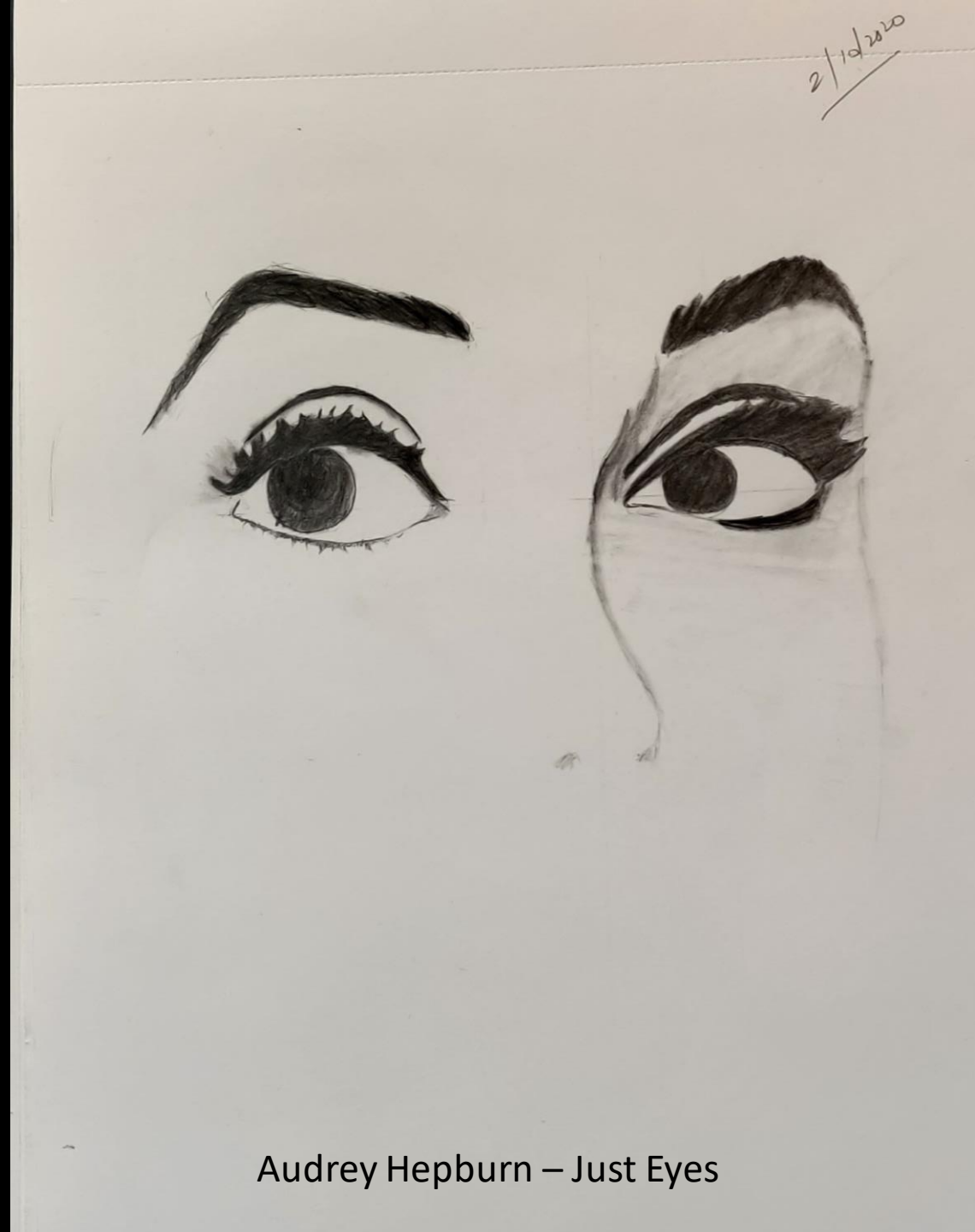
Enter in Amount: 8

Enter in Receiver Name: Janki

Enter in Nonce Value: 1

Submit

Created by Janki
Purchased by Utsav



Audrey Hepburn – Just Eyes

Enter in Sender Name: Meenakshy

Enter in Amount: 12

Enter in Receiver Name: Ravi

Enter in Nonce Value: 1

Submit

Created by Ravi
Purchased by Meenaskshy

Enter in Sender Name: Nikhil

Enter in Amount: 10

Enter in Receiver Name: Ravi

Enter in Nonce Value: 1

Submit

Created by Ravi
Purchased by Nikhil

Enter in Sender Name: Venkat

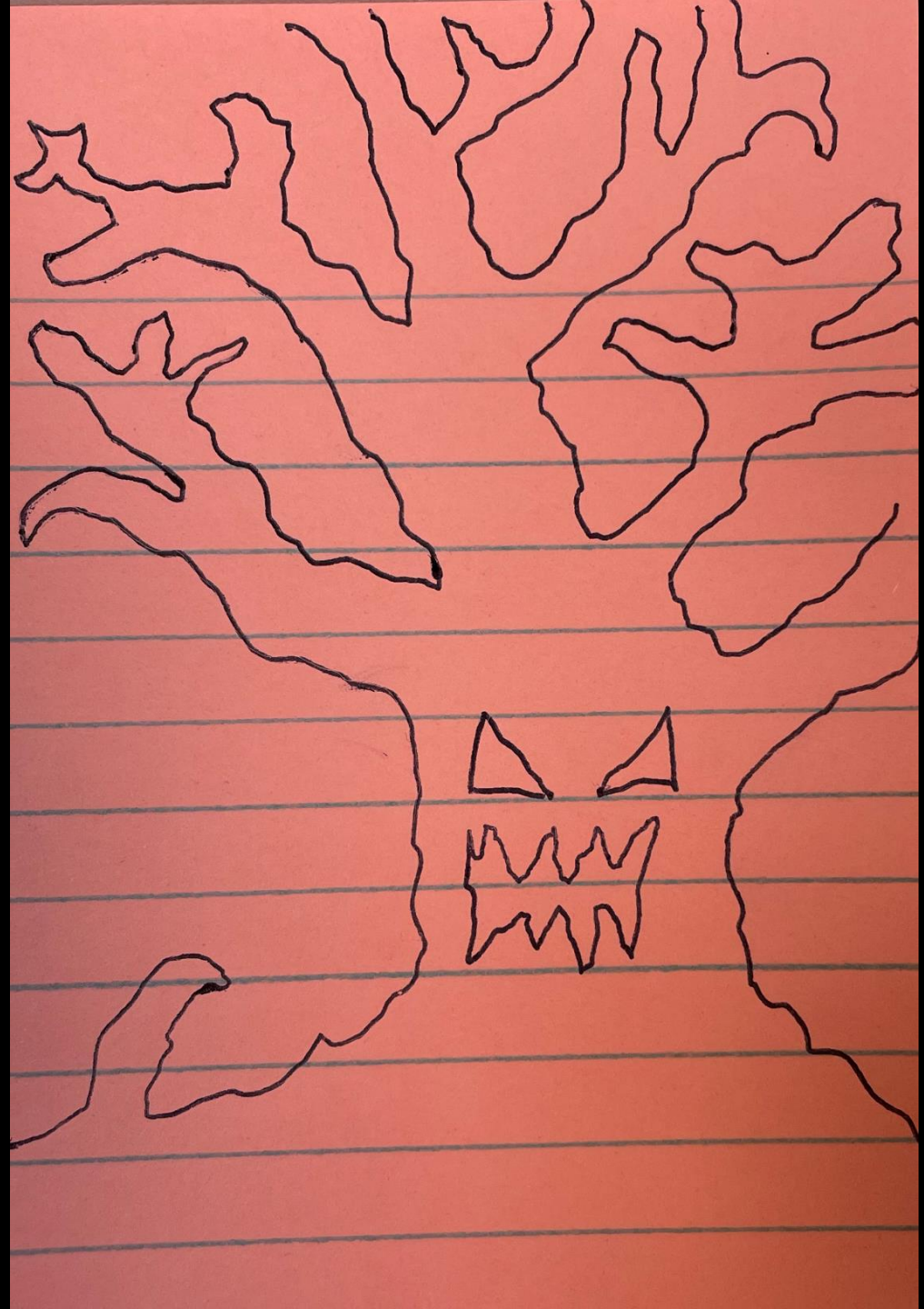
Enter in Amount: 18

Enter in Receiver Name: Mark

Enter in Nonce Value: 1

Submit

Created by Mark Houle
Purchased by Mudappallur Raman Venkateswaran



Enter in Sender Name: Shreya

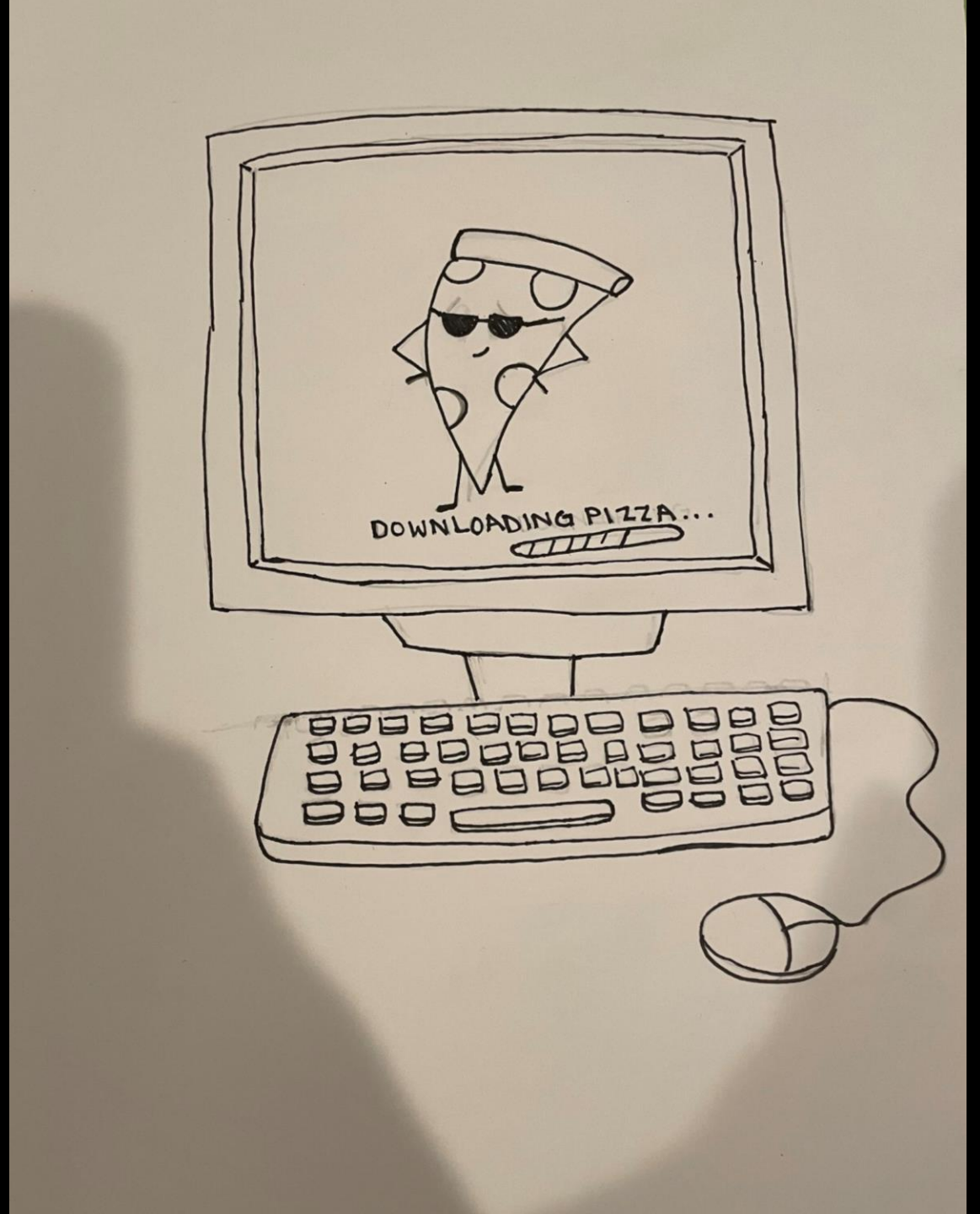
Enter in Amount: 19

Enter in Receiver Name: Sadie

Enter in Nonce Value: 1

Submit

Created by Sadie
Purchased by Shreya



Enter in Sender Name: Shreya

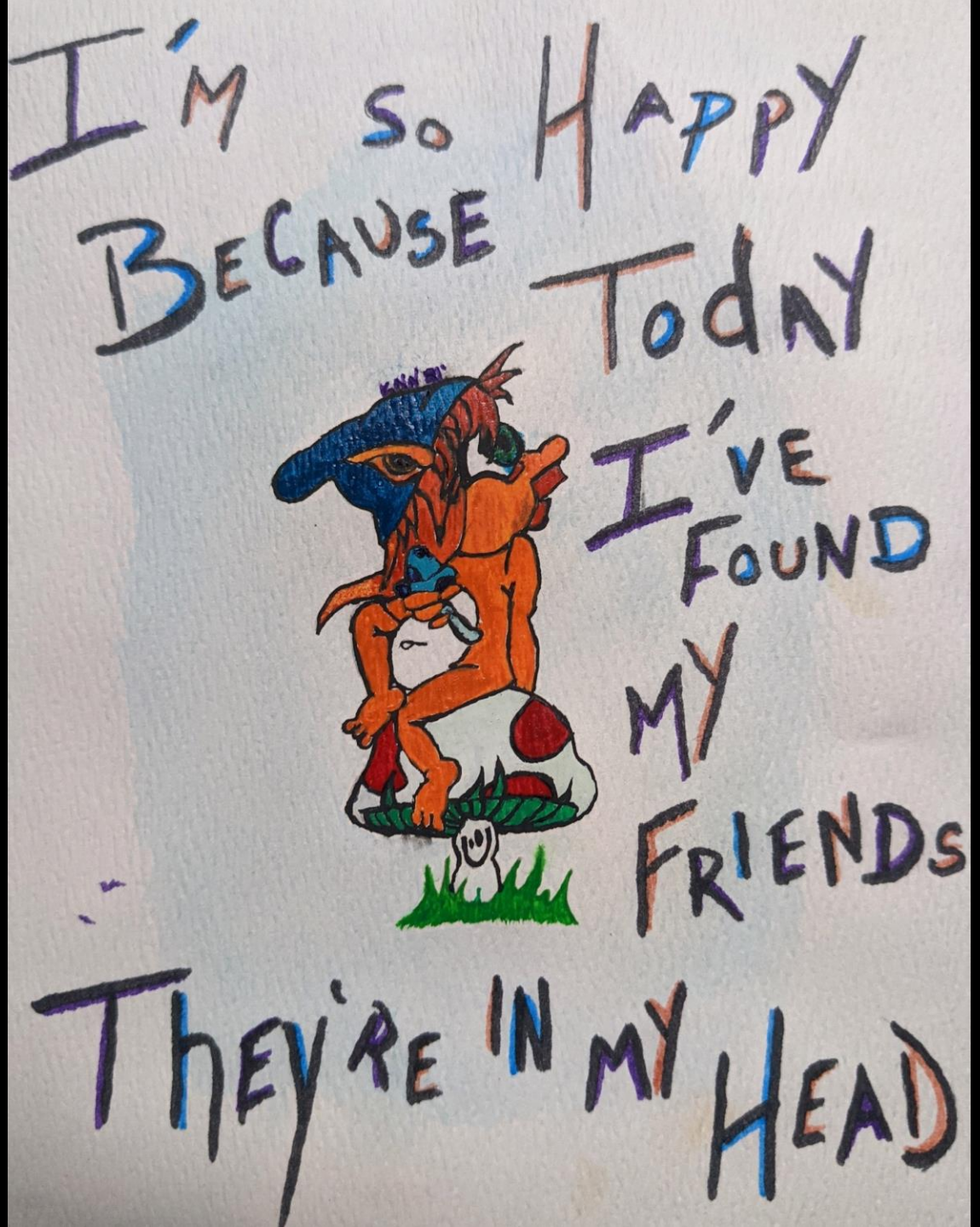
Enter in Amount: 15

Enter in Receiver Name: Kaylia

Enter in Nonce Value: 1

Submit

Created by Kaylia
Purchased by Shreya



Enter in Sender Name: Larry

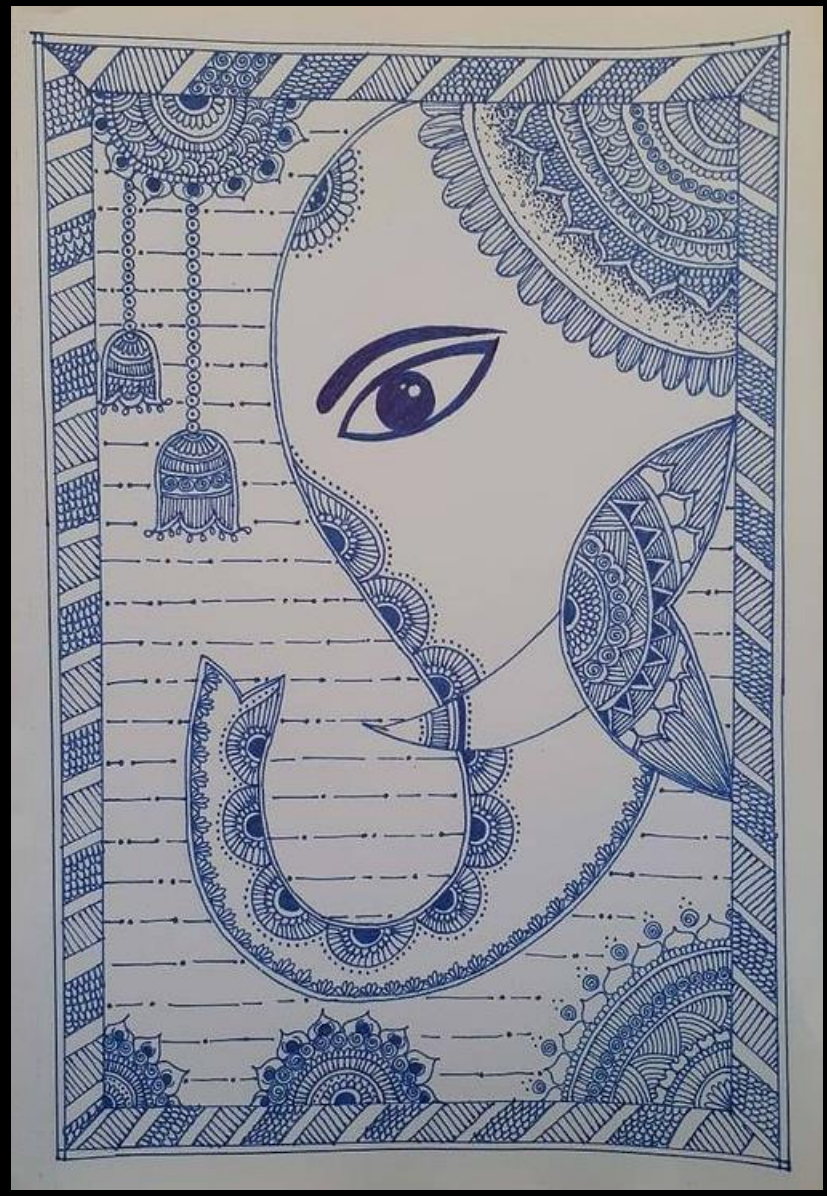
Enter in Amount: 20

Enter in Receiver Name: Sneha

Enter in Nonce Value: 1

Submit

Created by Sneha Tadakala
Purchased by Larry



Enter in Sender Name: Sania

Enter in Amount: 14

Enter in Receiver Name: Priya

Enter in Nonce Value: 1

Submit

Created by Priya
Purchased by Sania

Enter in Sender Name: Ayida

Enter in Amount: 10

Enter in Receiver Name: Priya

Enter in Nonce Value: 1

Submit

Created by Priya
Purchased by Ayida

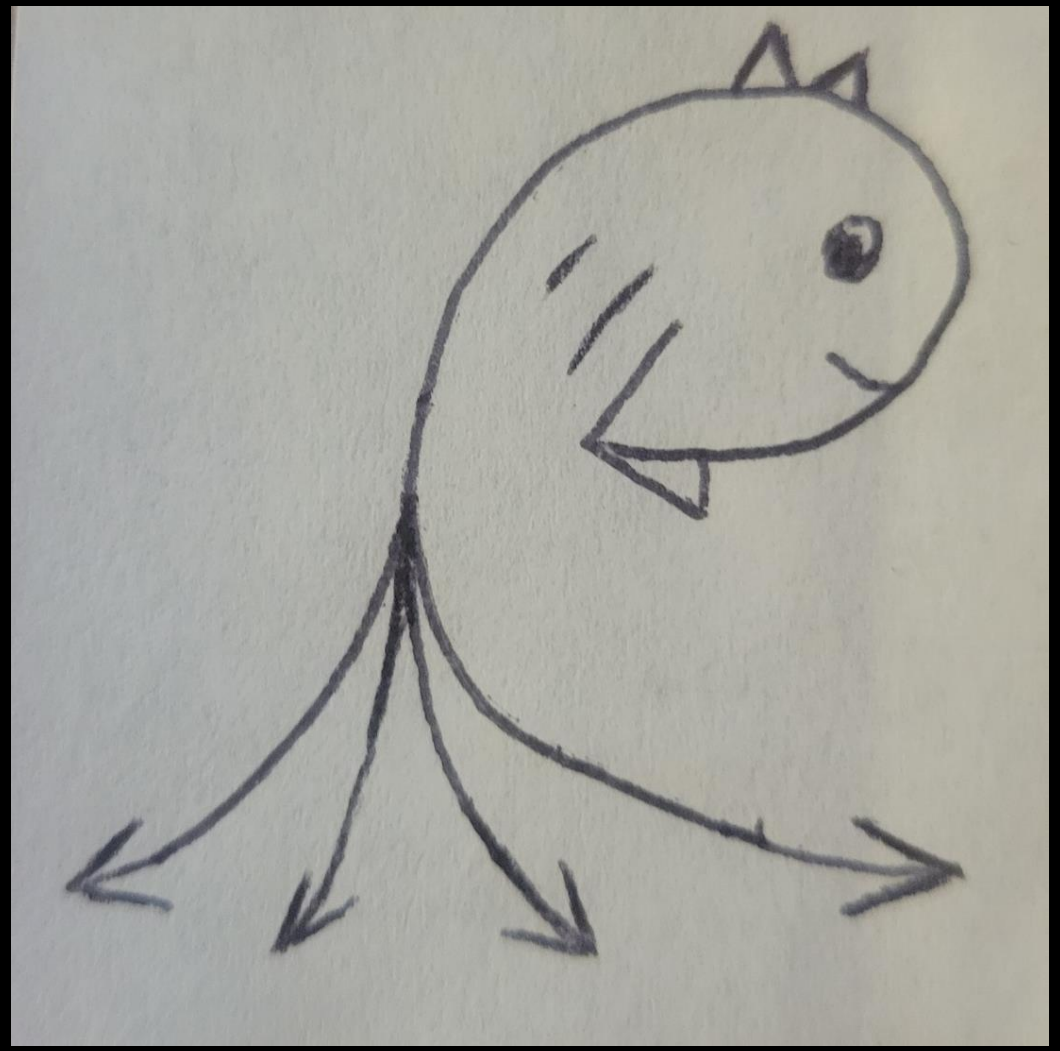
Enter in Sender Name: Nikhil

Enter in Amount: 15

Enter in Receiver Name: Jacob

Enter in Nonce Value: 1

Submit



Created by Jacob
Purchased by Nikhil

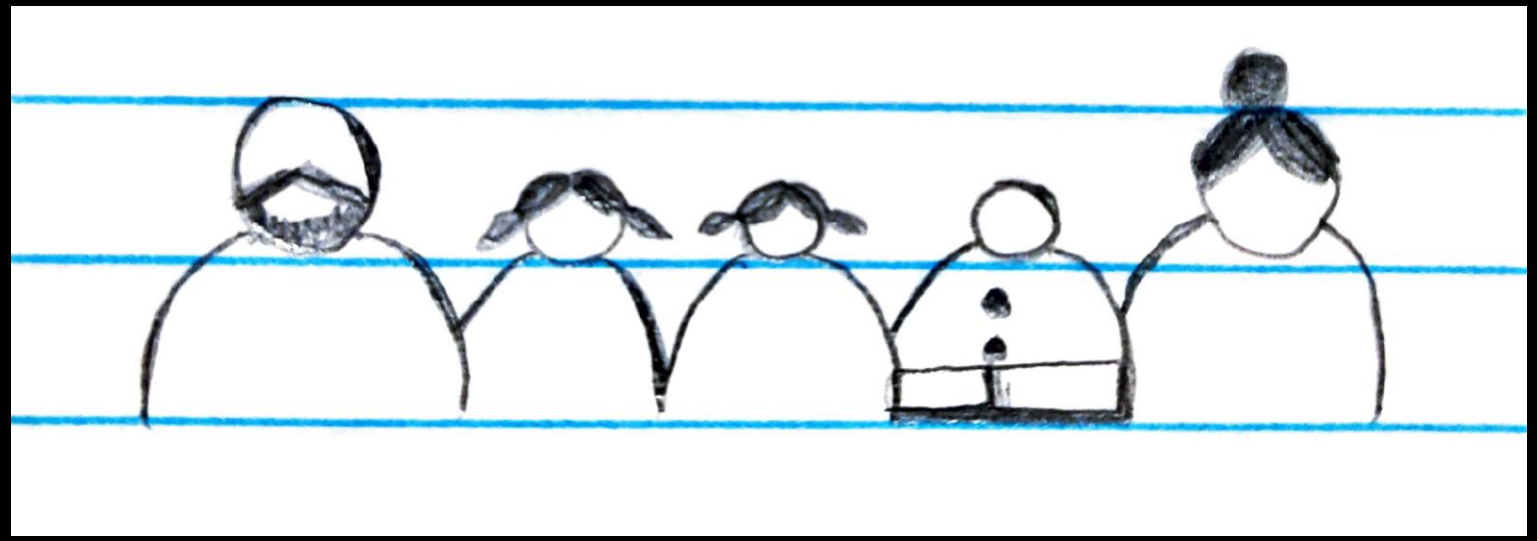
Enter in Sender Name: Ayida

Enter in Amount: 10

Enter in Receiver Name: Grishma

Enter in Nonce Value: 1

Submit



Created by Grishma
Purchased by Ayida

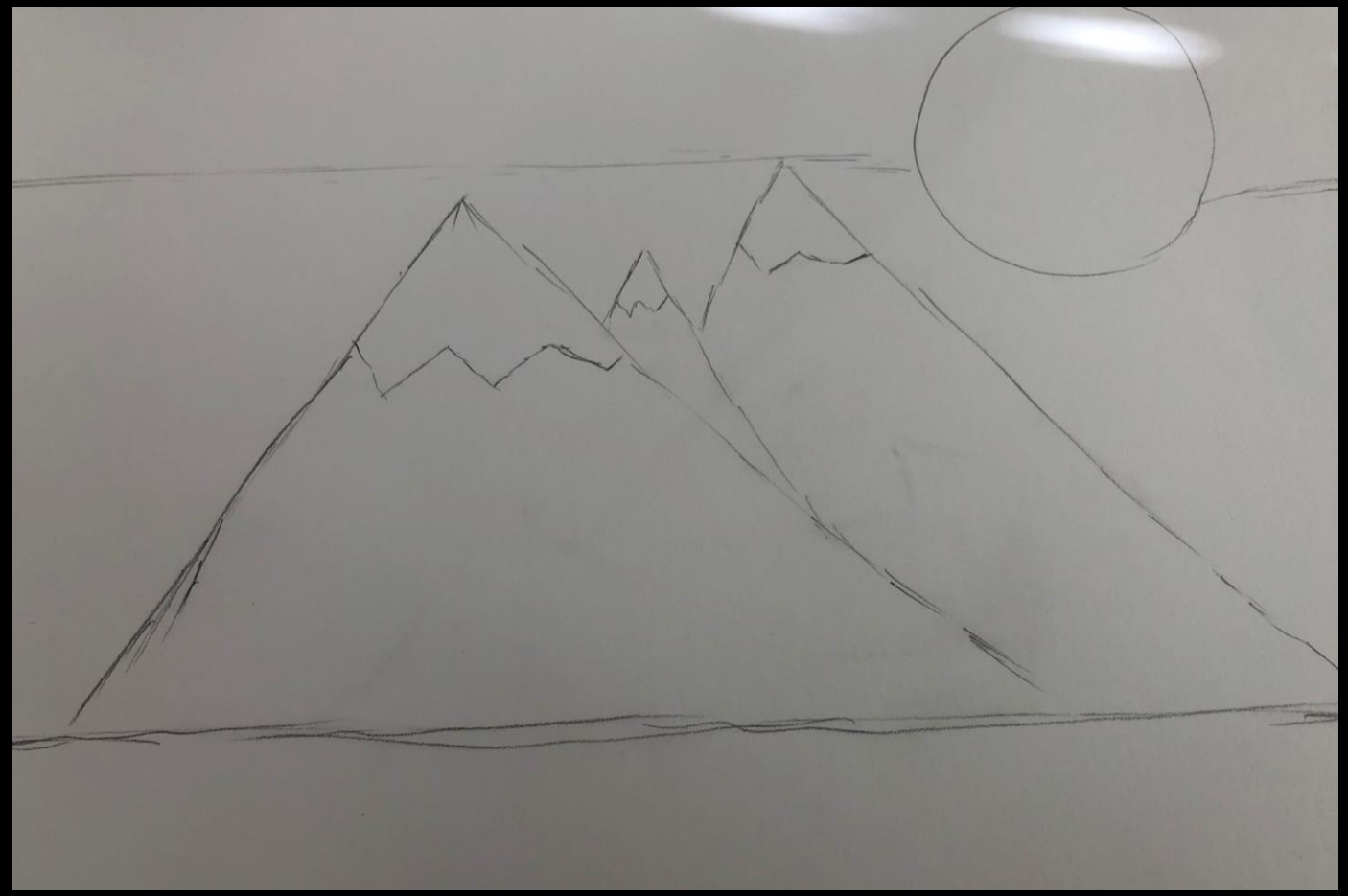
Enter in Sender Name: Jackie

Enter in Amount: 18

Enter in Receiver Name: Martin

Enter in Nonce Value: 1

Submit



Created by Martin Hutchison
Purchased by Jackie

Enter in Sender Name: Steve

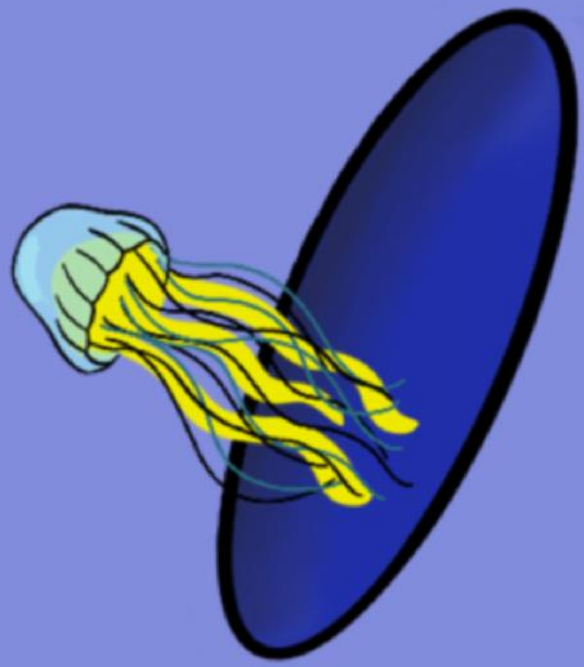
Enter in Amount: 25

Enter in Receiver Name: Josh

Enter in Nonce Value: 1

Submit

Created by Joshua Simmons
Purchased by Steve



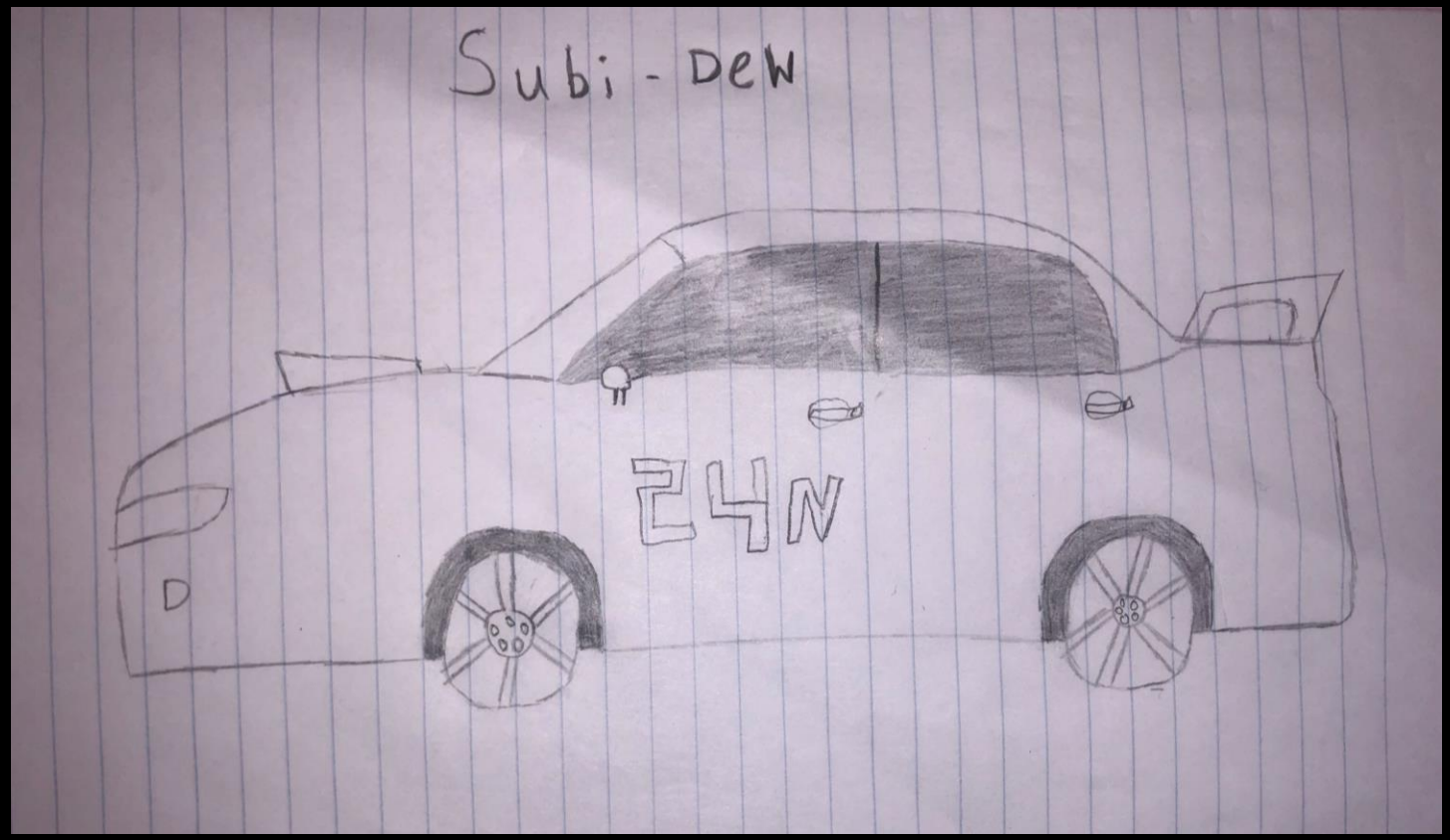
Enter in Sender Name: Jay

Enter in Amount: 20

Enter in Receiver Name: Dan

Enter in Nonce Value: 1

Submit



Created by Daniel Colasurdo
Purchased by Jay Lethin

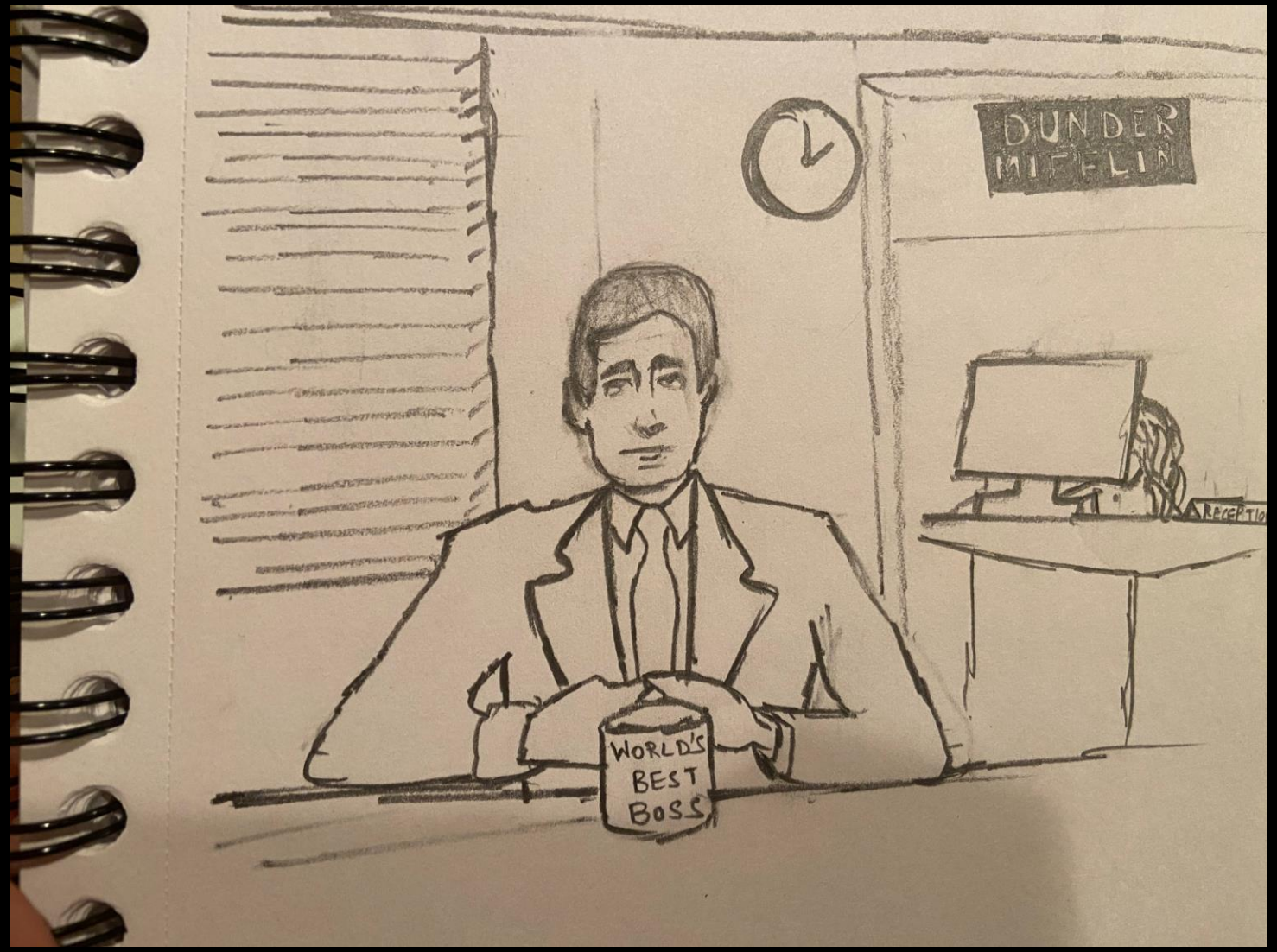
Enter in Sender Name: Eric

Enter in Amount: 3

Enter in Receiver Name: Richa

Enter in Nonce Value: 1

Submit



Created by Richa Gambhir
Purchased by Eric Liew

Enter in Sender Name: Aditi

Enter in Amount: 4

Enter in Receiver Name: Alyssa

Enter in Nonce Value: 1

Submit

Created by Alyssa Brouillet
Purchased by Aditi Katti

Enter in Sender Name: ????

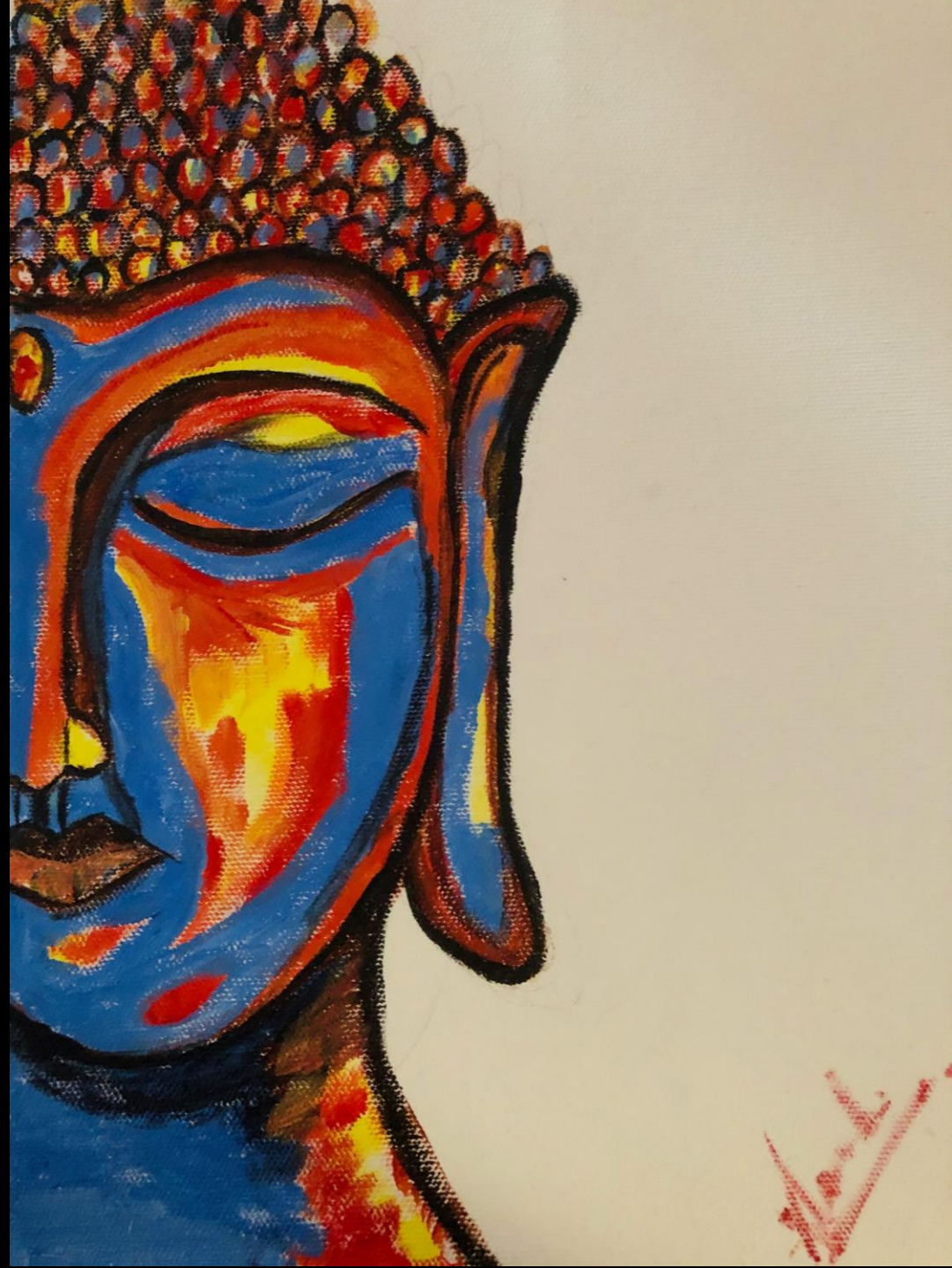
Enter in Amount: ?

Enter in Receiver Name: Sakshi

Enter in Nonce Value: 1

Submit

Created by Sakshi
Purchased by ????



Enter in Sender Name: ????

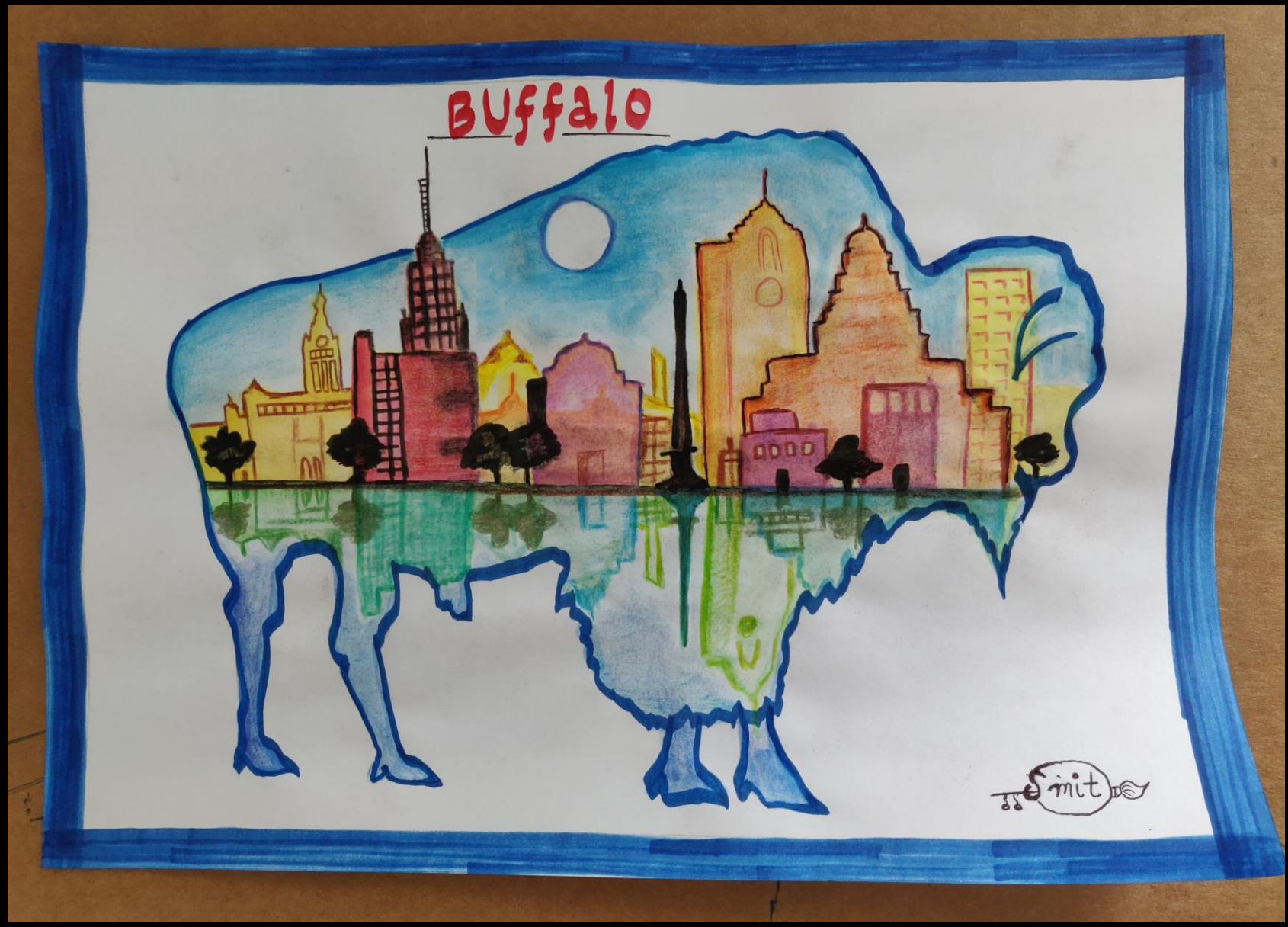
Enter in Amount: ?

Enter in Receiver Name: Smit

Enter in Nonce Value: 1

Submit

Created by Smit
Purchased by ????



Enter in Sender Name: ????

Enter in Amount: ?

Enter in Receiver Name: Kalyani

Enter in Nonce Value: 1

Submit

Created by Kalyani
Purchased by ????

Enter in Sender Name: Kanika

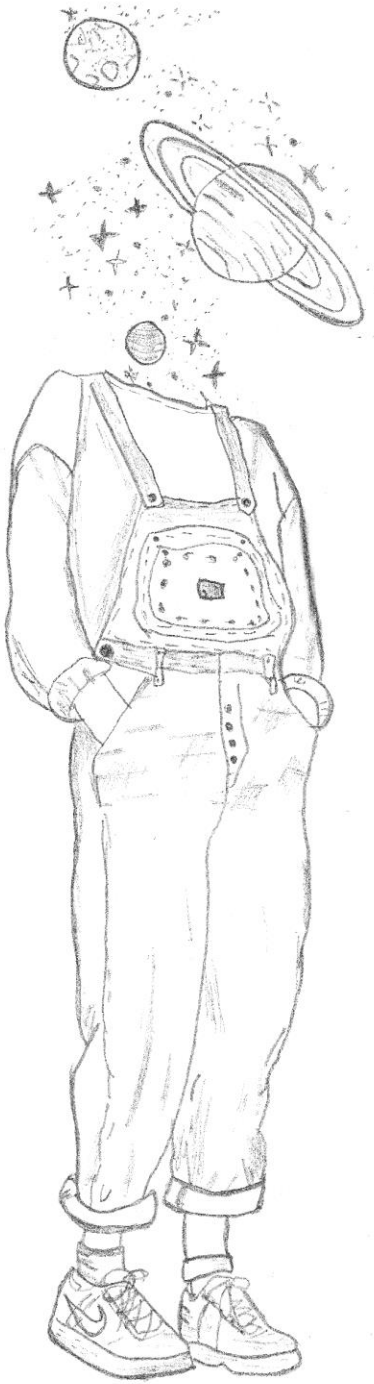
Enter in Amount: 5

Enter in Receiver Name: Mayuri

Enter in Nonce Value: 1

Submit

Created by Mayuri Garg
Purchased by Kanika Gulyani

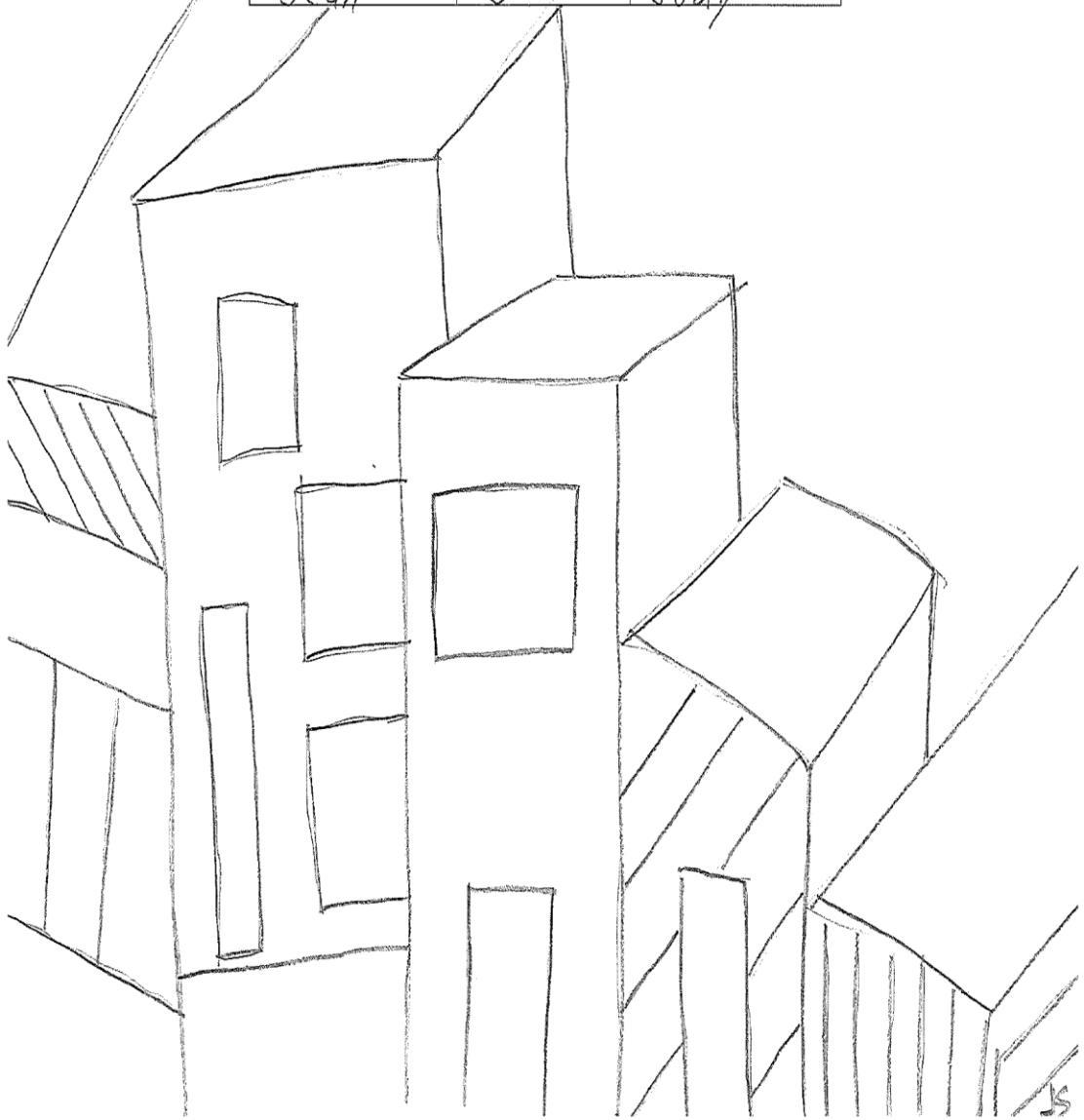


BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
Larry	4	Jody

BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
Sean	5	Jody



BARTS Drawing Transaction

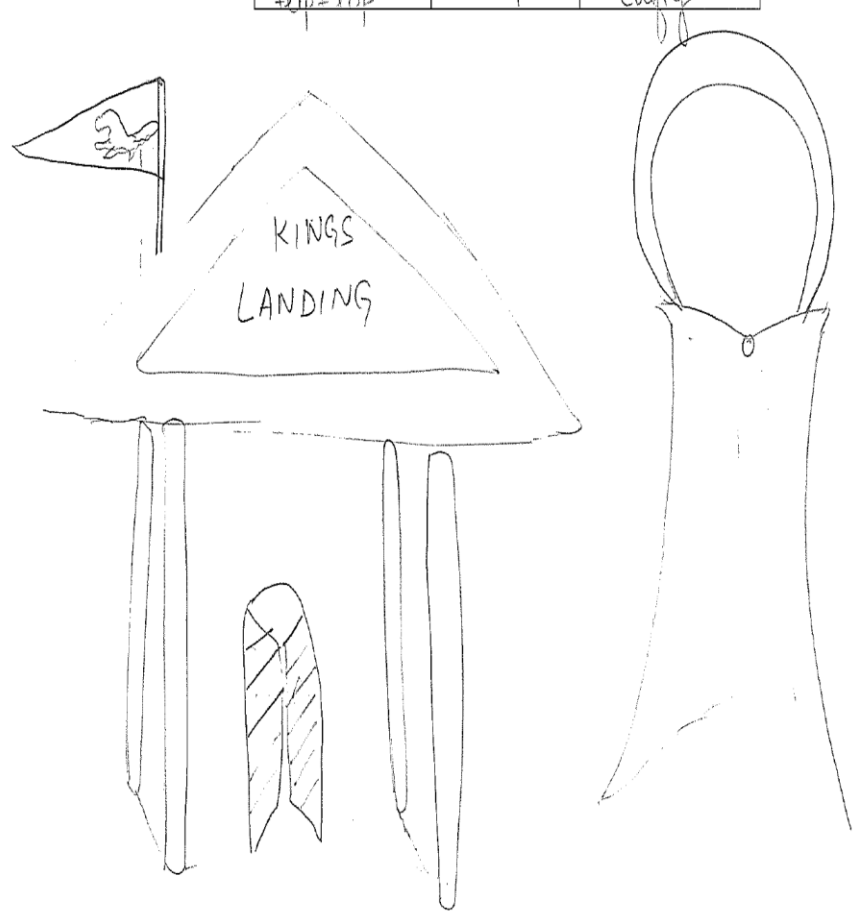
Buyer (Gallery)	Amount	Seller (Artist)
BoBo	4 Barts	CRAFTY

Bobo - 4

Flip-flop - 4

BARTS Drawing Transaction

Buyer (Gallery)	Amount	Seller (Artist)
Flip Flop	4	Crafty

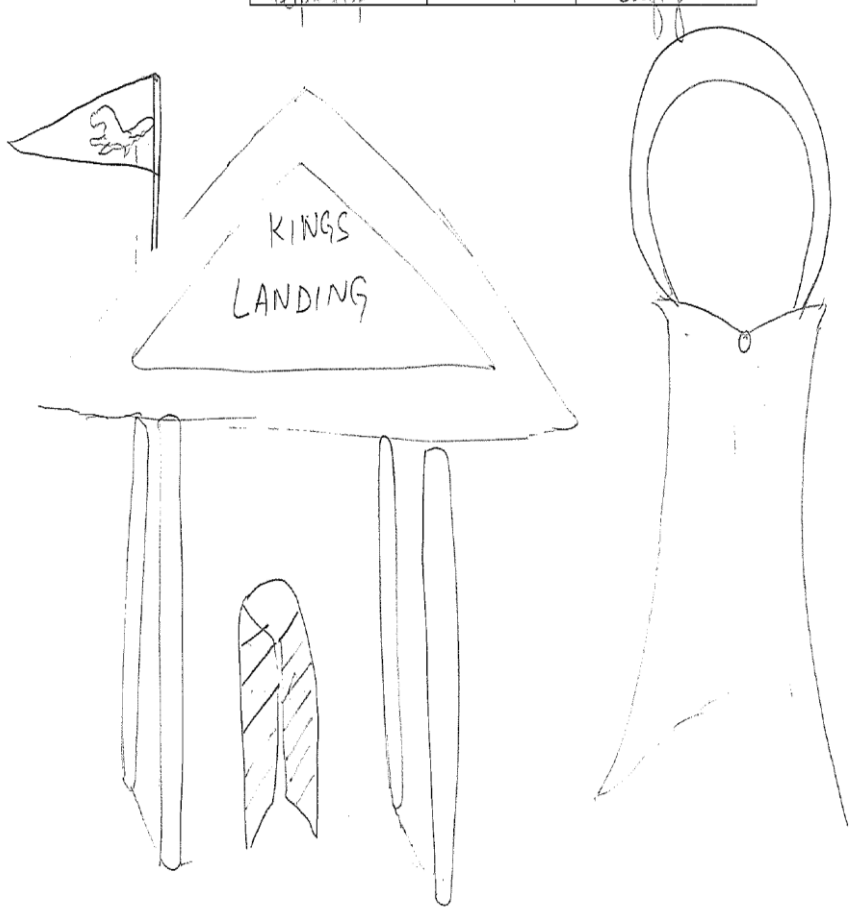


Bobo - 4

Flip Flop - 4

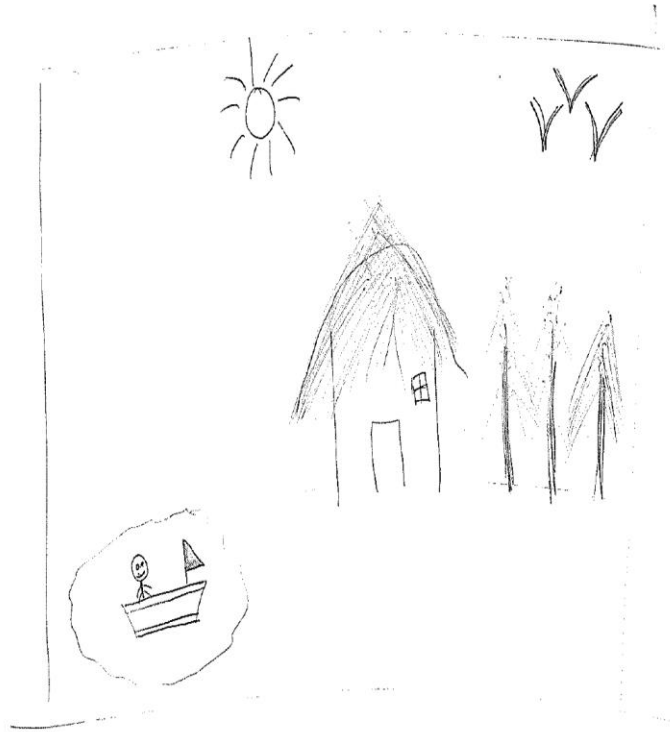
BARTS Drawing Transaction

Buyer (Gallery)	Amount	Seller (Artist)
Flip Flop	4	Goofy



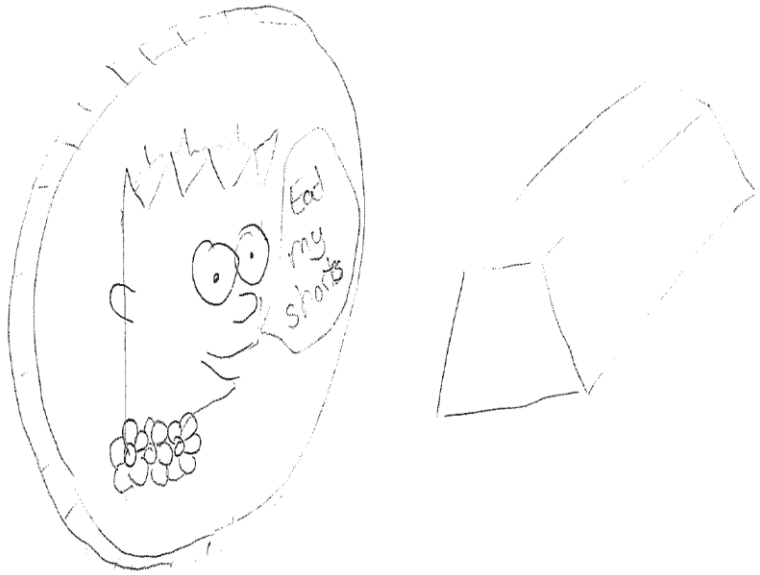
BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
Derek	Five	Sneha



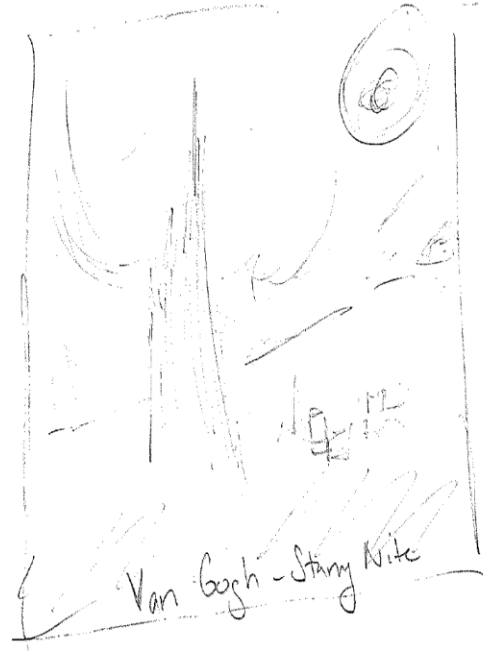
BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
Denise	2	Christina



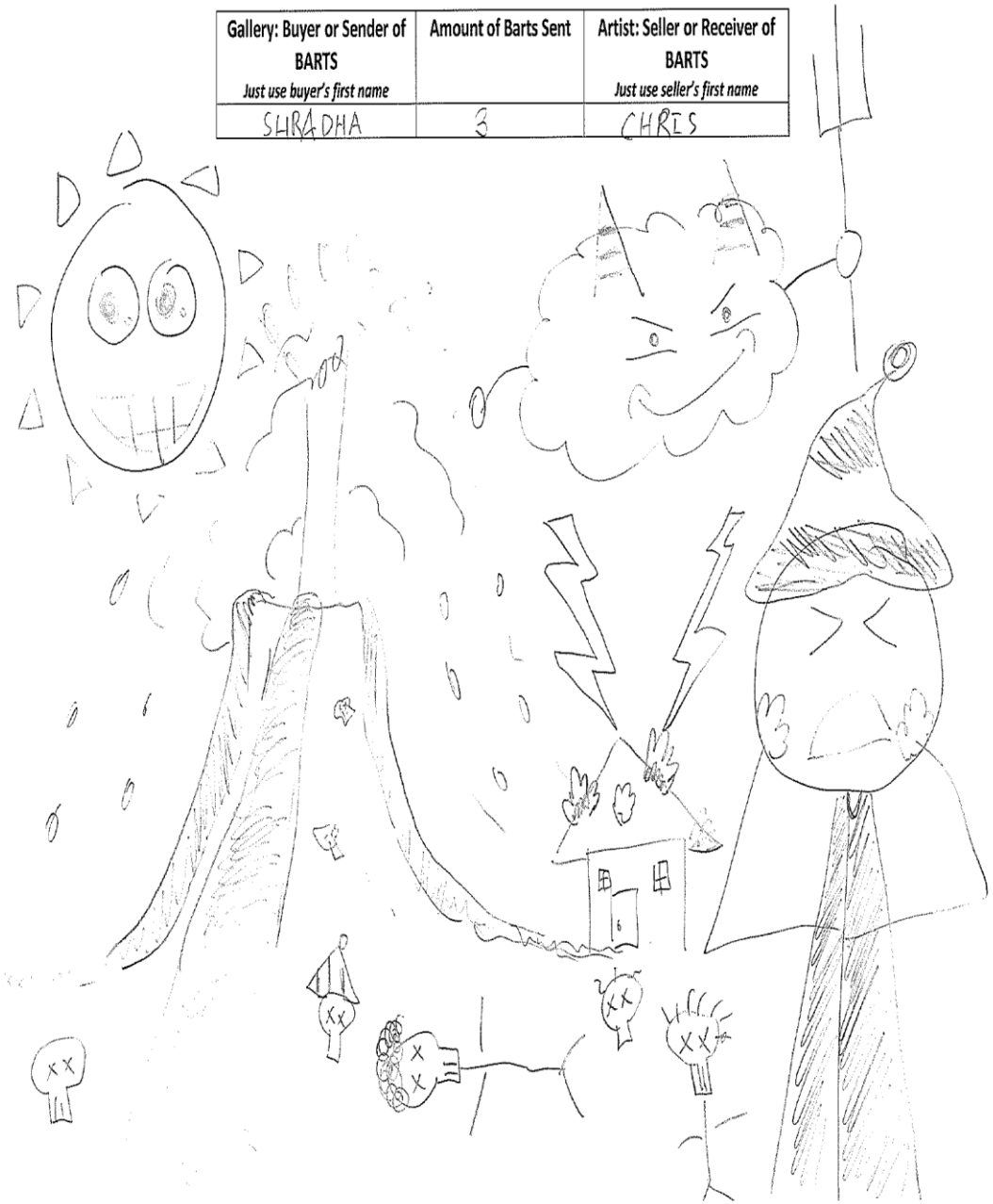
BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
Ivine	3	Suzanna



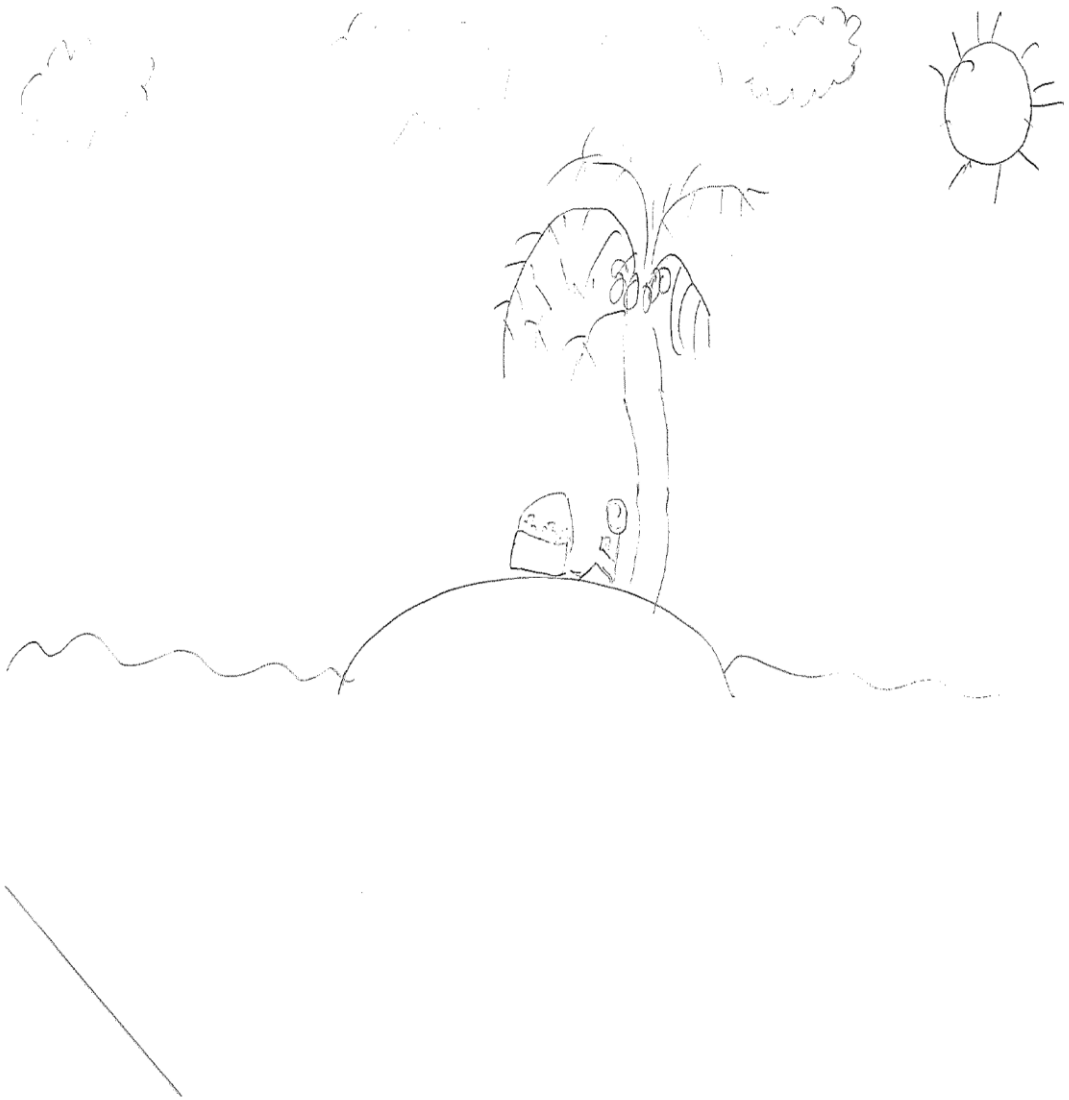
BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
SHRADHA	3	CHRIS



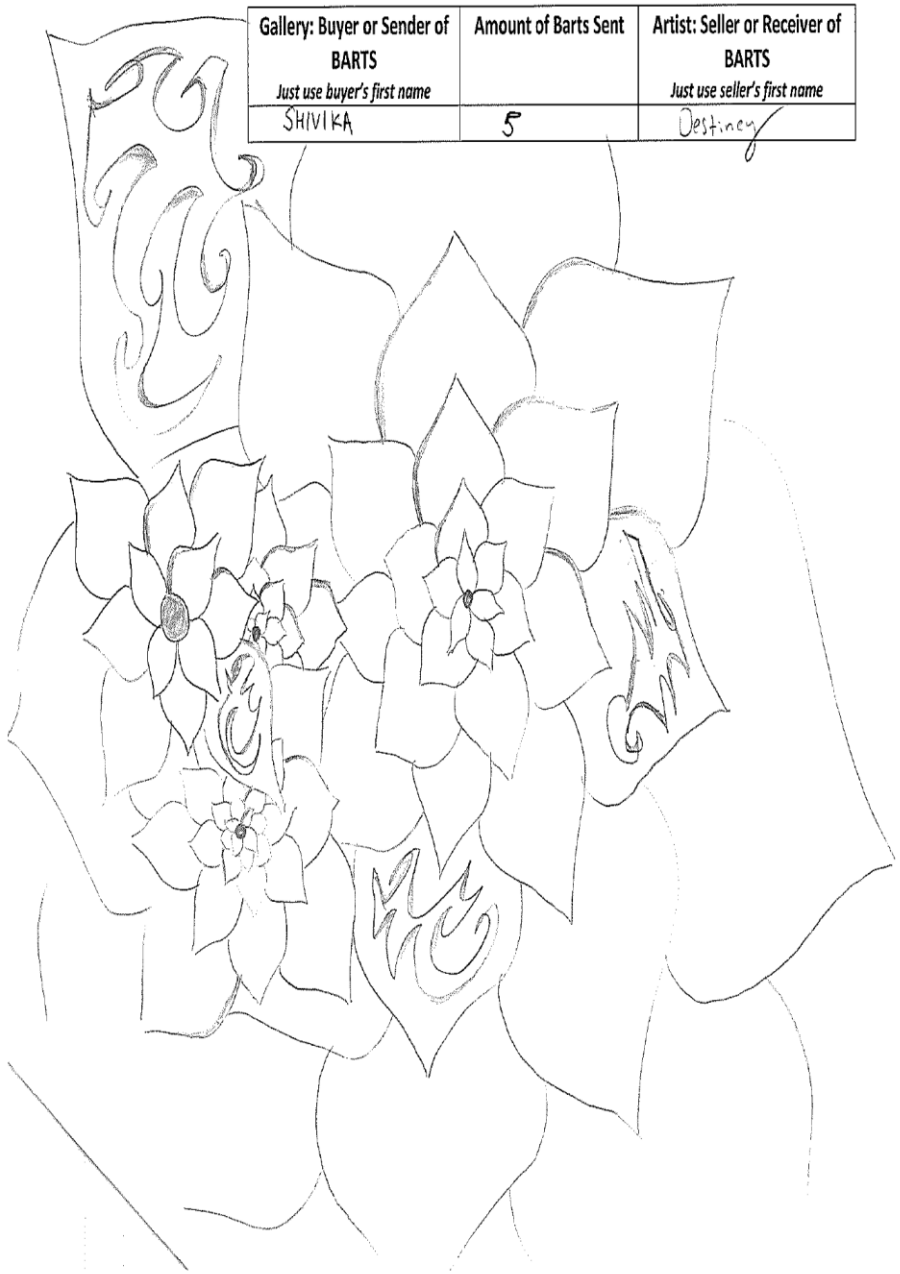
BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
Purva.	3	Macky



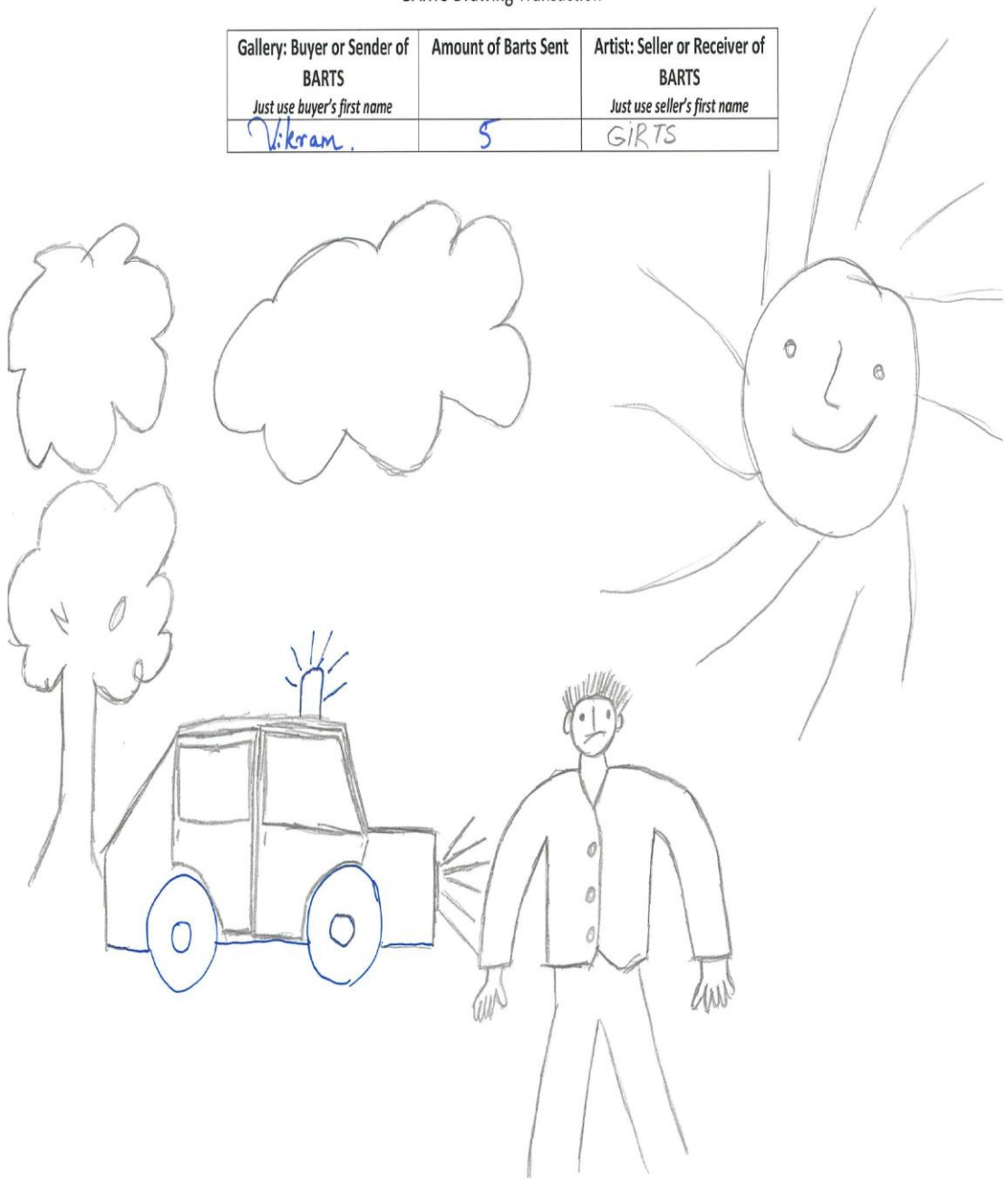
BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
SHIVIKA	5	Destiney



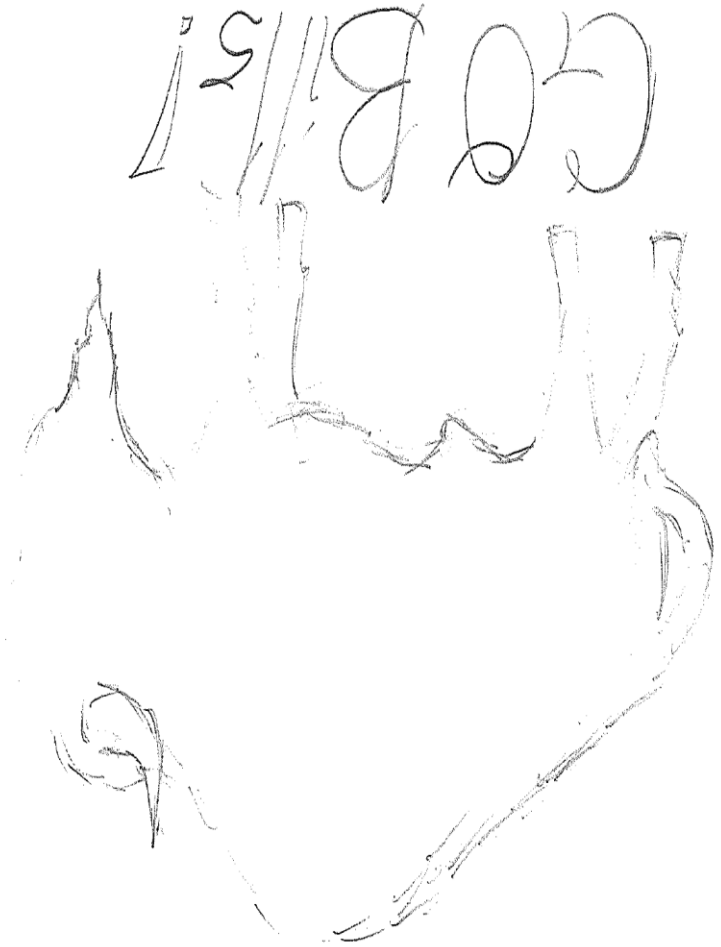
BARTS Drawing Transaction

Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
Vikram.	5	GIRTS

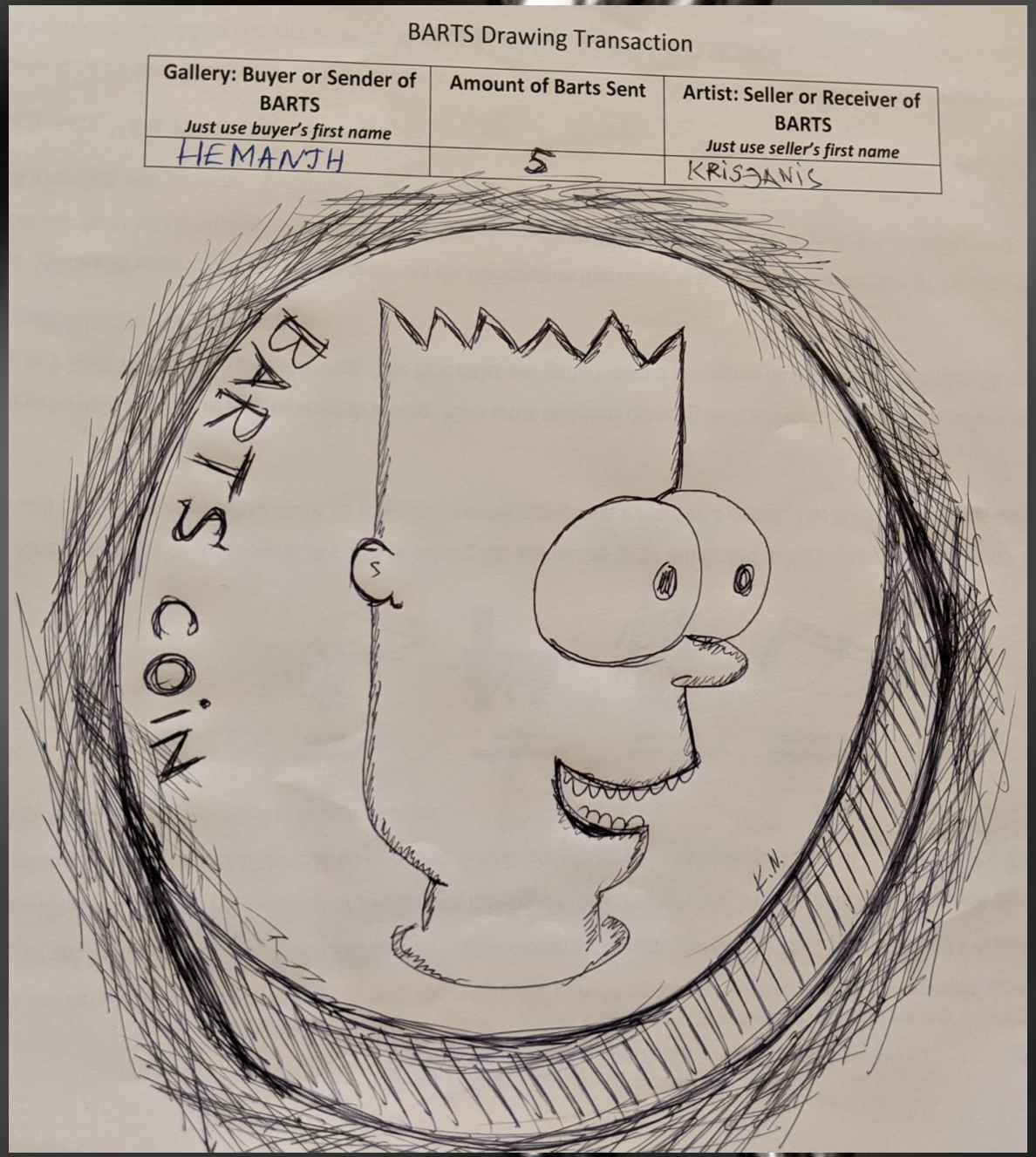


BARTS Drawing Transaction

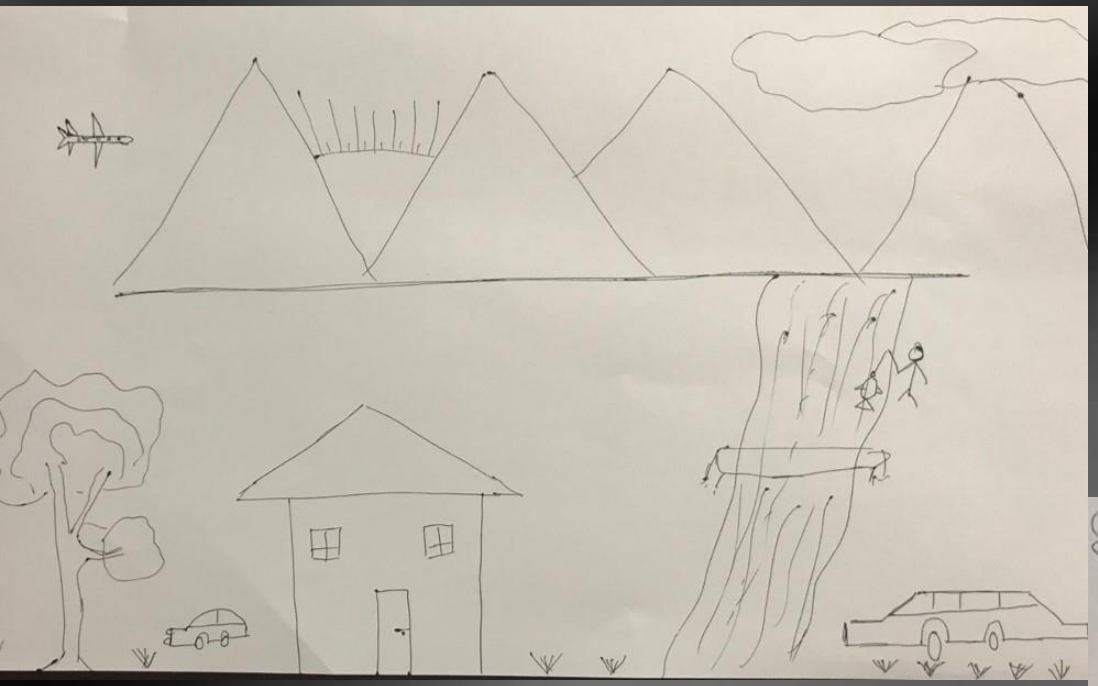
Gallery: Buyer or Sender of BARTS *Just use buyer's first name*	Amount of Barts Sent	Artist: Seller or Receiver of BARTS *Just use seller's first name*
Anubha	$5	Austin Bratek



This was mined at
a nonce value of 86



First Semester



Other Topics

- Money
- Experiential exercises on hashing
- Interesting applications of hashing
- NFTs Non fungible Tokens
- Smart Contracts

Thank you for your time

Additional material on Hashing:

- A set of four exercises were developed to illustrate hashing concepts.

- These exercises were first introduced at the 2018 North Eastern conference for the CSCC in Arlington Virginia by Sean Sanders. The paper received the best student paper award ("A-Nonce the Use and Performance of Hashing Algorithms)

Exercise 1: Generate a nonce that will result in a leading zero for a hash.

- Students enter their name with the number 1 right after their name. If the first character is not a zero, they keep incrementing the number following their name by one more unit until a hash with one leading zero is generated. This program is available at https://tinyurl.com/ZeroHashMining.

Exercise 2: A Hashing program that automatically searches for a nonce.

- This algorithm is quite complex because the program has to keep searching until it finds a hash with the correct number of leading zeros. This is what miners do for a living using specialized hardware using hash speeds of hashes to find a hash with 17 leading zeros. This program is written in PHP and is available at https://tinyurl.com/ZeroHashMining2.

Exercise 3: Mining Computation Issues

- The purpose of this exercise is to illustrate in greater detail the computational demand that is required for using hashing for proof of work.
- It requires participants to enter the text to be hashed, along with the number of leading zeros, then to click on the hashing algorithm desired and the number of times to run the simulation. The program will find the hash by adding a nonce, or random number, to the string until it generates a hash with the appropriate number of leading zeros. This program is available at https://tinyurl.com/ZeroHashMining3.

Mining Complexity

This is controlled by the number of leading zeros required

- Bitcoin mining for one block should take around 10 minutes.

- Hash with 1 zero requires about 16^{1} or 16 attempts.
- Hash with 2 zeros requires about 16^{2} or 256 attempts.
- Hash with 3 zeros requires about 16^{3} or 4,096 attempts.
- Hash with 4 zeros requires about 16^{4} or 65,536 attempts.
- Hash with 5 zeros requires about 16^{5} or 1,048576 attempts.
- Hash with 17 zeros requires about 16^{17} or 2.9514791e+20 attempts.

Exercise 3: Output

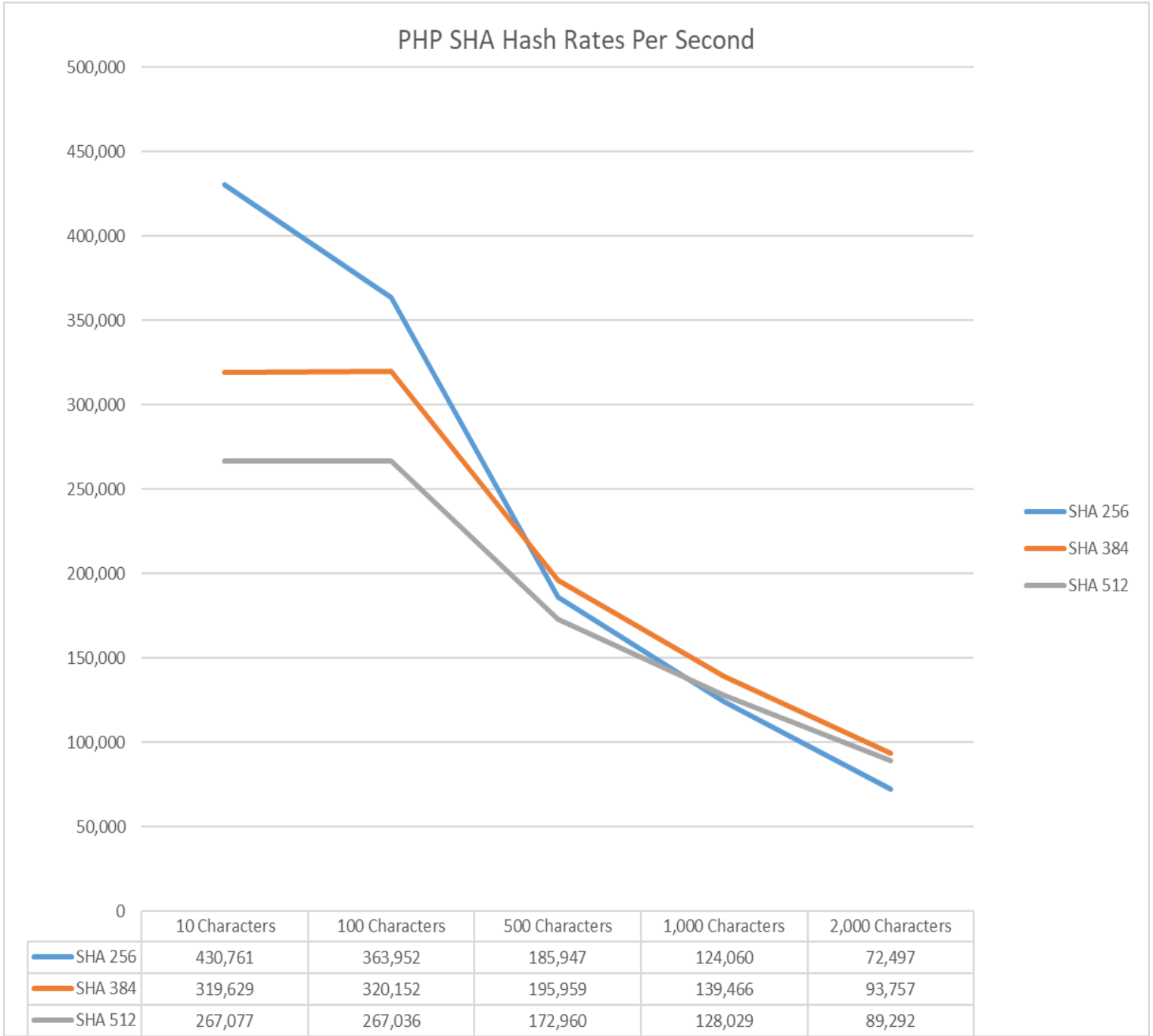
Results from Mining Simulation

Your Sentence is: John Doe CIS
Your sentence length is: 12
Zeros to account for is: 4
Nonce value is: 933,449,540
The initial hash of the sentence without Nonce is: e4fcc0ca29e6c094daf393550cd44bca3f97d2aede7be9b3fb0511434748dcb5
You picked SHA-256 **for the hash algorithm**

Number of Attempts	Time in Seconds	Hash Rate
70,422	0.16	440,137.500
10,698	0.03	356,600.000
21,017	0.05	420,340.000
56,672	0.13	435,938.462
60,458	0.14	431,842.857
61,141	0.14	436,721.429
93,395	0.22	424,522.727
173,599	0.41	423,412.195
90,083	0.21	428,966.667
7,769	0.02	388,450.000
Average Attempts	Average Time	Average HashRate
64,525	0.151	418,693.180

Using the above simulation

- It can be used to understand how the number of leading zeros translates to computational intensity. The average number of attempts is a function of the number of leading zeros and is $16^{\wedge n}$ where n is the number of leading zeros.
- Students can simulate the performance of the various algorithms and copy the results into a spreadsheet. These results can then be used to write a short paper that discusses the results.
- The figure on the next page was constructed by cutting and pasting the results from running the simulation 100 times for all three hash functions, by varying the number of characters from 10 through 2,000. About 76,838,804 million hashes were used to generate these results. The projected number of hashes to compute was 78,643,200.
- Between 1,000 and 2,000 transaction are hashed in each Bitcoin block.



	10 Characters	100 Characters	500 Characters	1,000 Characters	2,000 Characters
SHA 256	430,761	363,952	185,947	124,060	72,497
SHA 384	319,629	320,152	195,959	139,466	93,757
SHA 512	267,077	267,036	172,960	128,029	89,292

Cryptographic hash functions have these important security properties

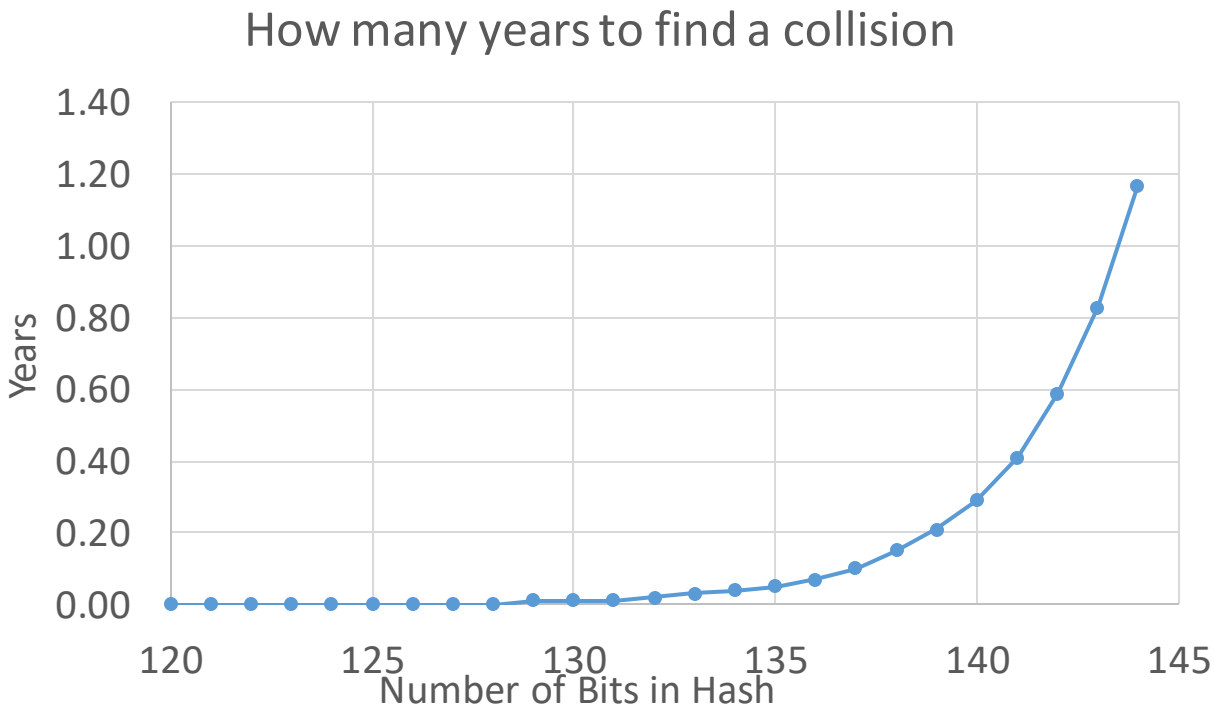
1. "**They are preimage resistant.** Preimage resistance is one component of the hash function that is difficult to turn. If a hash function within the range of an element is given, it is expected to be computationally infeasible to locate the input that matches such element."
2. **They are second preimage resistant. "**Second preimage resistance, which is also one of the hash function properties, can be referred to as "weak collision resistance." This property can be infeasible when it is computed, which makes it difficult to locate the input of the second distinct that has the same output as the given input."
3. **They are collision resistant**. "Collision resistance also has similarities with the second preimage resistance, and because of this, collision resistance can also be called "weak collision resistance." However, before a hash function can be referred to as collision resistance, it must have a minimum of 160 bits length."

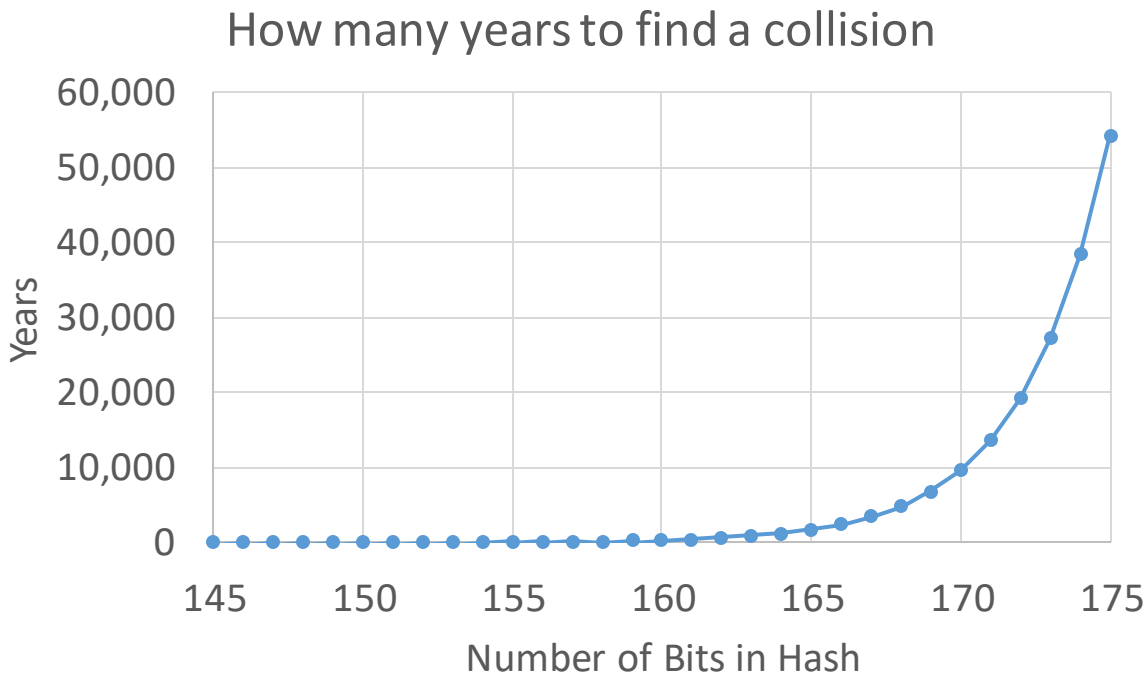
https://freemanlaw.com/preimage-resistance-second-preimage-resistance-and-collision-resistance/

Exercise 4: Birthday Paradox and cracking secure hash algorithms

- The safety of secure hash algorithms is always an issue of interest. The Birthday Paradox can be used as an approximation of the amount of brute force computing necessary to find a hash collision. The program used to illustrate the number of years to find a hash Collison for various SHA bit sizes and hash rates can be found at https://tinyurl.com/BirthdyaParadoxExample.
- For example, the number of years needed to find a collision for the lowly 160 bit SHA1 algorithm using 5,000 ASICS computers each capable of 13TH/s with a total hashing rate of 65,000 TH/s, is 0.74 years. This is in contrast to the 208.06 trillion years to find a collision with the SHA256 algorithm using the brute force approach.

Years to find a collision from 120 bits to 175 using 160 TH/s





Summary

- Hashing is the key to mining.
- The blockchain is a powerful secure tool for storing data.
- In some form, blockchain will be part of our future.
- Just like Zoom, Facebook, Tiktock, Instagram, Venmo, and Robinhood.

Hashing Applications

- Secure hash algorithms are used to verify that data has not been altered, such as in:
  - Man-in-the-middle: This is where an attacker sits between two parties and monitors or alters communication.
  - Password protection: Passwords are usually stored as hashes .
  - Digital signatures: Electronic fingerprints ensure that message contents have not been changed during transport.
  - File verification: Hashes used to ensure file has not been altered. Can also be used to identify and track malware.

Benefits of BARTS

- Anonymous surveys sent in December 2020 and April 2021 to 125 graduate students. We asked the students about the percentage of the new understanding of hashing concepts they received from the teaching module? The mean for the knowledge and understanding increase was 73.6%.

Table 1: Effectiveness of blockchain materials

Questions	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
The material covered in the Blockchain Arts Simulation (BARTS) helped me gain a clearer understanding of blockchain concepts	4 (4.2)%	2 (2.1%)	4 (4.2%)	40 (41.7%)	46 (47.9%)
The material covered in the module related to hashing gave me gain a clearer understanding of blockchain concepts	3 (3.1)%	2 (2.1)%	4 (4.2%)	40 (41.7%)	47 (49.0%)

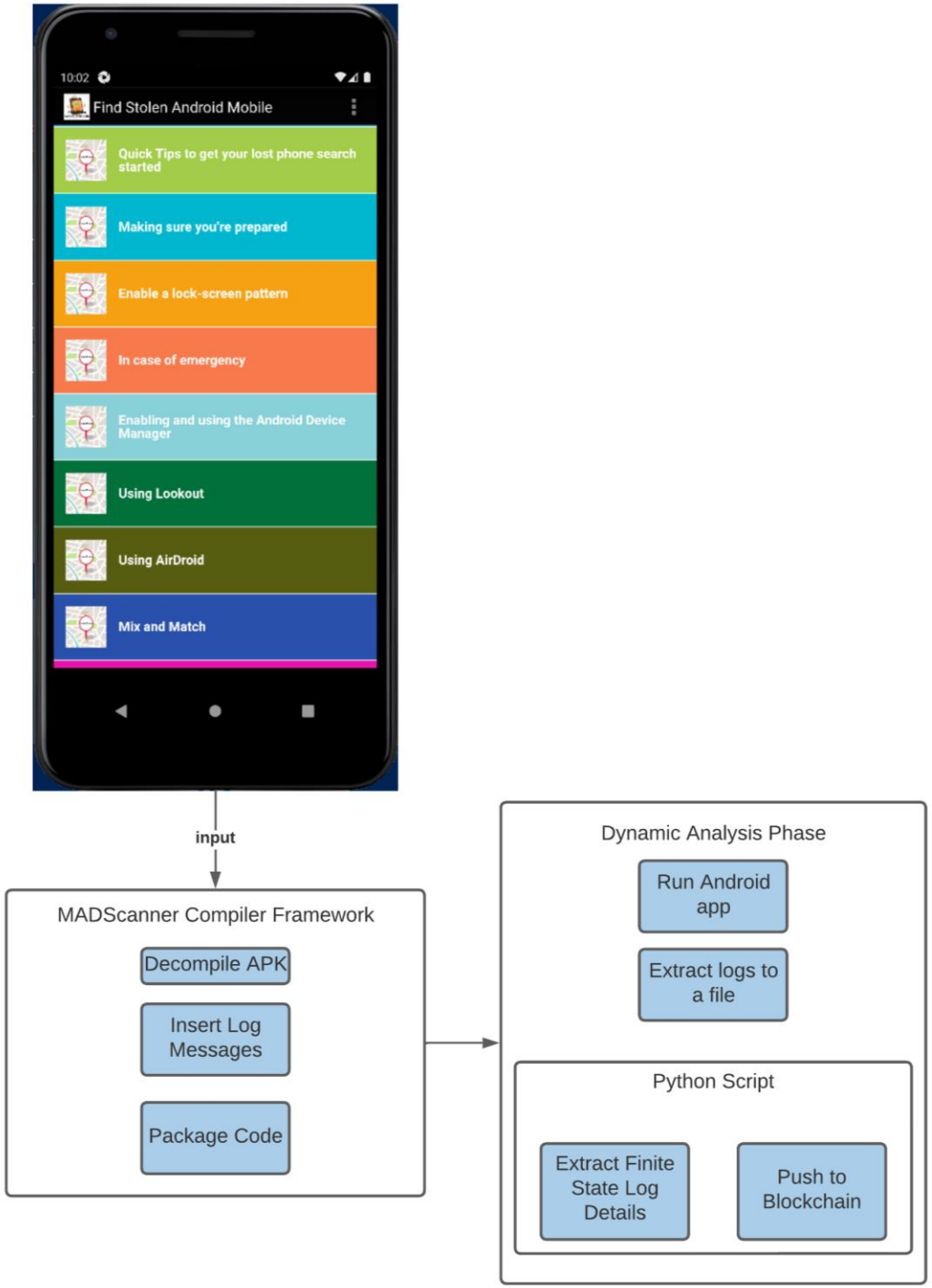
Blockchain Teaching Module Materials

250 to 500 hours of prep for three * 1 ½ class hours

- Blockchain Art Simulation
- A set of four exercises were developed to illustrate hashing concepts.
- Maersk: Betting on Blockchain case: https://www.maersk.com/apa-tradelens
- Overview of fiat currency versus cryptocurrency
- The outcome
  - Students like the material
  - At least two or three of the groups in the Technology and Innovation Management course design a blockchain application.
  - Two papers at HICSS
  - Dissertation

Mobile Advertisement Scanner(MADScanner)

1. Decompile the Android APK
2. Analyze the ADMob Library calls
3. Insert log messages after ADMob library calls
4. Compile and package the Android APK
5. Run the Android application
6. Log details are sent to the Ethereum blockchain
7. Log details in the blockchain are compared against the Finite State Machine Model.


10:02
Find Stolen Android Mobile
Quick Tips to get your lost phone search started
Making sure you're prepared
Enable a lock-screen pattern
In case of emergency
Enabling and using the Android Device Manager
Using Lookout
Using AirDroid
Mix and Match
input
MADScanner Compiler Framework
Decompile APK
Insert Log Messages
Package Code
Dynamic Analysis Phase
Run Android app
Extract logs to a file
Python Script
Extract Finite State Log Details
Push to Blockchain

The Real End

BARTS Players

- Coordinator or instructor
- Artists
- Gallery Owners & Buyers
- Mining Pools with several miners in each pool.

Coordinator

1. Artists complete a drawing on a Bart's sheet for negotiated price.

2. The gallery owner takes the completed Bart's diagram to the coordinator.

3. The coordinator asks the mining pool to validate the Bart's transaction after determining if the gallery owner has sufficient number of Barts.

4. The mining pool hashes the transaction.

5. The mining pool that finds the hash with the correct number of leading zeros tells the coordinator they have found the hash.

6. The coordinator announces what nonce to use that will generate the hash with correct number of leading zeros.

7. All of the mining pools validate the transaction with the nonce.

8. If the mining pools validate the hash, then the Bart's sheet is put up on the front wall and the ledgers are all updated by the mining pools.

Mining Pool

Mining Pool

Mining Pool

Bitcoin Mining in Tonawanda at Digihost

- https://digihost.ca/docs/what-we-do/
- https://digihost.ca/docs/charts/


Bitcoin Mining
https://www.youtube.com/watch?v=jxXn1bPtLdE

Hashing & Mining

- Hashing algorithms are used to verify digital currency transactions and then to add them to the distributed blockchain ledger.

- A **mining pool** is a group of miners that join forces to combine computing power. Large mining pools increase the chance for successful hashing. The current block reward for successful mining is 6.25 Bitcoins. The block reward is halved after 210,000 blocks have been processed.

- An decrease in mining success for new entrants is related to the presence of large mining companies and consortia with deep pockets.

- An increase in mining success for new entrants can also be related to a reduction in hashing power. China put a halt to some of the mining in China June of 2021.

BARTS and Experiential Exercises

- Many people, not just computer science students, find blockchain concepts, in particular mining concepts, to be elusive.
- We have found that the answer requires a modest understanding of **hashing.**
- The existing material on blockchain concepts tends to be either simplistic or technically complex and there are not enough hands-on exercises.
- Our goal with this material is to address this issue.

Typical Block Statistics for Mining

On June 29, 2021 there were around one million Bitcoin miners performing 100 million trillion hashes over a 24 hour period to find a hash for Block 689129 with 19 zeros. Here are the block statistics

Block 689129

This block was mined on June 29, 2021 at 7:54 AM EDT by F2Pool. It currently has 1 confirmations on the Bitcoin blockchain. The miner(s) of this block earned a total reward of 6.25000000 BTC ($221,190.44). The reward consisted of a base reward of 6.25000000 BTC ($221,190.44) with an additional 0.16437477 BTC ($5,817.30) reward paid as fees of the 2482 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 936.09069495 BTC ($33,128,689.66) were sent in the block with the average transaction being 0.37715177 BTC ($13,347.58). Learn more about how blocks work.

Hash 000000000000000009b3e5ac9ba06474bad6b48c1d701977bdb03e90d18ef7

Potential Benefits of blockchain

- There is greater **trust** because banks and government our taken out of the picture. Fewer intermediaries
- There are multiple groups and people that have a copy of the ledger of accounts. The ledger is **distributed.**
- The ledger of accounts containing the previous transactions and status of ownership is **identical**.
- The ledger of accounts is **immutable**. This means the ledger cannot be changed once written.
- Blockchain transactions are **secure** because of encryption and password protection.

BITCOIN WHALES

- INDIVIDUALS OWNING AT LEAST 100 BITCOINS.
  - HTTPS://BLOG.COINSOURCE.NET/WHO-OWNS-THE-MOST-BITCOIN/

Collisions from NISTIR

- “Since there are an infinite number of possible input values and a finite number of possible output digest values, it is possible but highly unlikely to have a collision where hash(x) = hash(y) (i.e., the hash of two different inputs produces the same digest). SHA-256 is said to be collision resistant, since to find a collision in SHA-256, one would have to execute the algorithm, on average, about 2128 times (which is 340 undecillions, or more precisely 38 340,282,366,920,938,463,463,374,607,431,768,211,456; roughly 3.402 x 10).

- To put this into perspective, the hash rate (hashes per second) of the entire Bitcoin network in 2015 was 300 quadrillion hashes per second (300,000,000,000,000,000/s) [7]. At that rate, it would take the entire Bitcoin network roughly 35,942,991,748,521 (roughly 3.6 x 1013) years2 to manufacture a collision (note that the universe is estimated to be 1.37 x 1010 years old)3. Even if any such input x and y that produce the same digest, it would be also very unlikely for both inputs to be valid in the context of the blockchain network (i.e., x and y are both valid transactions).”

Just for interest:
Potential Hash Computations

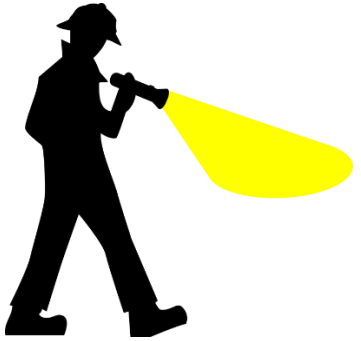
- Number of possible hashes when current hash must contain 1 leading zero. Probability that a randomly picked hash is a valid hash
  - 16^63/16^64 = 16^-1 = .0625

- Number of possible hashes when current hash must contain 17 leading zeros. Probability that a randomly picked hash is a valid hash
    - 16^47/16^64 = 16^-17 ~ 3.3881318e-21

Preventing Man-in-the-Middle Attack with Hashes

Original text prepared by secret agent is hashed

Man-in-the Middle attacker alters text



Receiving secret agent compares the two hashed values

Can we meet at Grand Central Station at 1pm?

Can we meet at Pier 11 at 1am?

SHA 256 Hash algorithm

Hash of text sent by attacker 83ac24b400caeb …

Check to see if hashes are the same

SHA 256 Hash algorithm

Hash of text sent by different route 4ccab6eec0e973 …

SHA256 Value of several common passwords that could be put in a password cracker dictionary. The user ids here are GOT baby names

User ID	Password	Hashed Value
Arya	123456	2c43c95d0f764aaea9a7ce3caa48803725a887f48cb3472b7087b0ba8ed98805
Tyrion	password	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
Brienne	12345678	ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f
Jorah	qwerty	65e84be33532fb784c48129675f9eff3a682b27168c0ea744b2cf58ee02337c5
Sansa	12345	5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc5
Catelyn	123456789	b0837559f9c780da799214524dc2dde7228c29c89e61f33e37aa1e8d14a82819
Ellaria	letmein	1c8bfe8f801d79745c4631d09fff36c82aa37fc4cce4fc946683d7b336b63032
Oberyn	1234567	8bb0cf6eb9b17d0f7d22b456f121257dc1254e1f01665370476383ea776df414
Theon	football	6382deaf1f5dc6e792b76db4a4a7bf2ba468884e000b25e7928e621e27fb23cb
Gregor	iloveyou	e4ad93ca07acb8d908a3aa41e920ea4f4ef4f26e7f86cf8291c5db289780a5ae
Sandor	admin	8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
Khal	welcome	280d44ab1e9f79b5cce2dd4f58f5fe91f0fbacdac9f7447dffc318ceb79f2d02
Daenarys	monkey	000c285457fc971f862a79b786476c78812c8897063c6fa9c045f579a3b2d63f

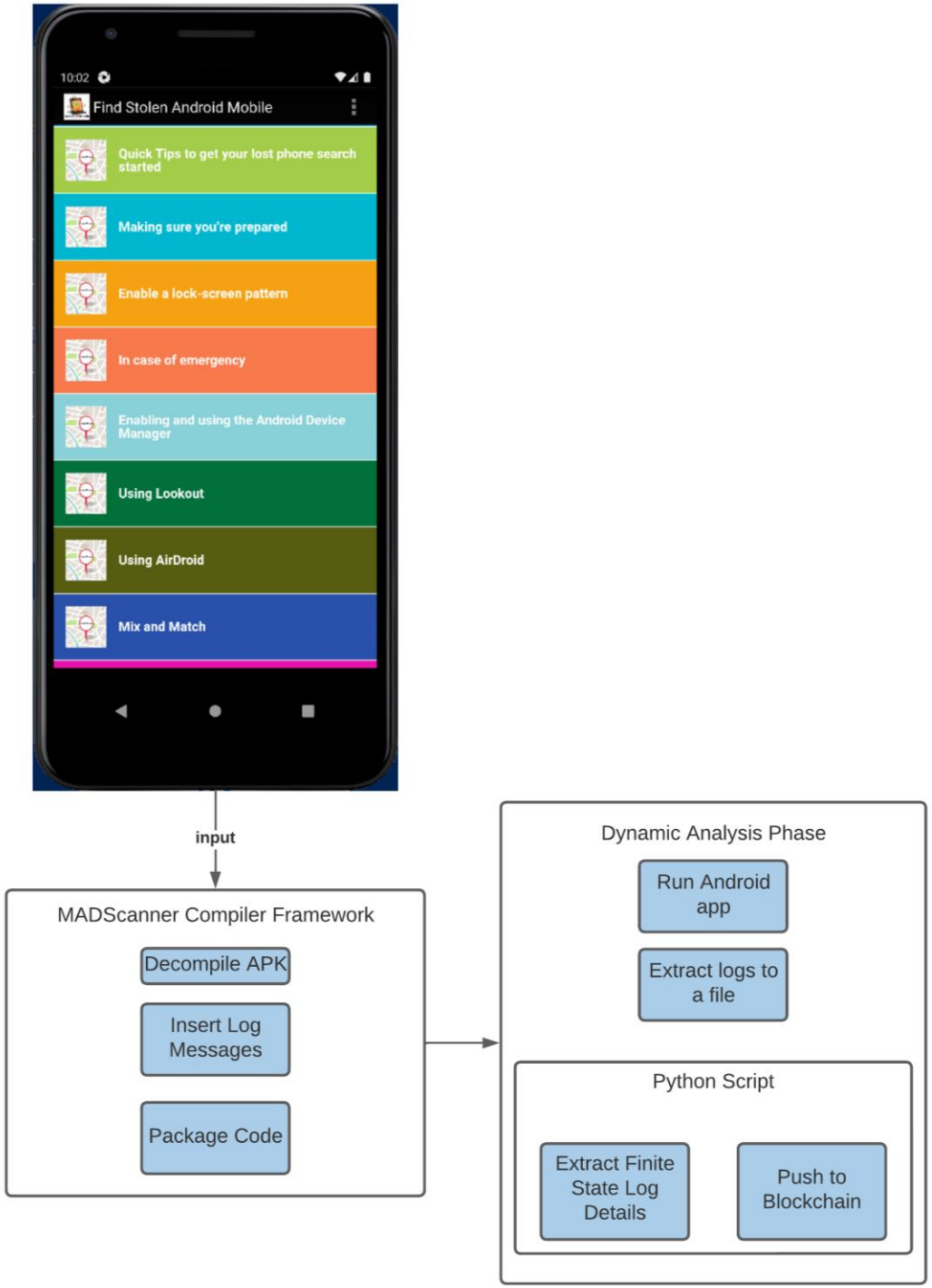
Adding Salt to Hashing: A Better Way to Store Passwords

- A cryptographic salt is made up of random bits added to each password instance before its hashing.
- Salts create unique passwords even in the instance of two users choosing the same passwords.
- Salts help us mitigate hash table attacks by forcing attackers to re-compute them using the salts for each user.
- Creating cryptographically strong random data to use as salts is very complex and it's a job better left to leading security solutions and providers.

Password	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

Mobile Advertisement Scanner(MADScanner)

1. Decompile the Android APK
2. Analyze the ADMob Library calls
3. Insert log messages after ADMob library calls
4. Compile and package the Android APK
5. Run the Android application
6. Log details are sent to the Ethereum blockchain
7. Log details in the blockchain are compared against the Finite State Machine Model.


10:02
Find Stolen Android Mobile
Quick Tips to get your lost phone search started
Making sure you're prepared
Enable a lock-screen pattern
In case of emergency
Enabling and using the Android Device Manager
Using Lookout
Using AirDroid
Mix and Match
input
MADScanner Compiler Framework
Decompile APK
Insert Log Messages
Package Code
Dynamic Analysis Phase
Run Android app
Extract logs to a file
Python Script
Extract Finite State Log Details
Push to Blockchain

Oreilly: Mastering Bitcoin

- The blockchain data structure is an ordered, back-linked list of blocks of transactions. The blockchain can be stored as a flat file, or in a simple database. The Bitcoin Core client stores the blockchain metadata using Google's LevelDB database. Blocks are linked "back," each referring to the previous block in the chain. The blockchain is often visualized as a vertical stack, with blocks layered on top of each other and the first block serving as the foundation of the stack. The visualization of blocks stacked on top of each other results in the use of terms such as "height" to refer to the distance from the first block, and "top" or "tip" to refer to the most recently added block.

- Each block within the blockchain is identified by a hash, generated using the SHA256 cryptographic hash algorithm on the header of the block. Each block also references a previous block, known as the parent block, through the "previous block hash" field in the block header. In other words, each block contains the hash of its parent inside its own header. The sequence of hashes linking each block to its parent creates a chain going back all the way to the first block ever created, known as the genesis block.
- https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html