Blockchain

1- Overview

Public-key cryptography uses a public and private key to encrypt messages.

This system can be used to verify messages by creating a unique signature that can be verified by anybody.

This process is the basis for transactions on blockchain networks, where individuals exchange currency without needing to trust one another.

In this activity, you will use a widget to simulate several blockchain transactions, including mining blocks and adding them to the shared blockchain ledger.

2- Vocabulary

Match the words to their definition:
Public Key ; Ledger ; Symmetric Encryption ; Encryption ; Message Signature ; Proof of Work ; Nonce ; Asymmetric Encryption ; **Key ; Mining ; Consensus** ; **Private Key ; Decryption** ; **Message Hash**

Vocabulary Term	Definition
	When different keys are used to encrypt and decrypt a message
	A mechanism requiring enough people to agree which transactions are valid
	Unscrambling a message to make it readable
	Scrambling or changing a message to hide the original text
	A secret password for unlocking a message
	A record of all transactions in a group
	a unique representation of an original message that has been transformed so it is unrecognizable.
	A unique encrypted message used to verify the sender of a message.
	When you continually generate new numbers to try and get a hash to start with a unique set of 0's. This is a puzzle that can only be solved by guessing
	A number used to try and change the hash of a block of messages so that it starts with a unique set of 0's. It's an abbreviation for "Number used once"
	A key that is kept private so only a specific person can decrypt a message
	Verifying information with a lot of computing effort
	A key that is shared with everybody so anyone can encrypt a message
	When the same key is used to encrypt and decrypt a message

3- Verifying Signatures

The blockchain helps facilitate thousands of transactions each day between people who've never met or trust each other.

Cryptographic signatures help verify that the person is actually who they say they are.

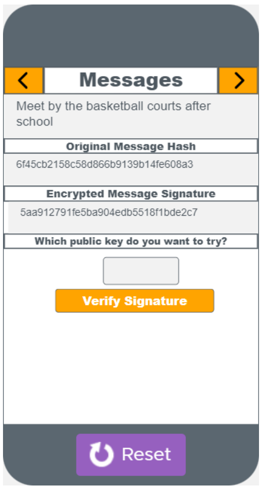
https://www.youtube.com/watch?v=Ssw63fBF20g

Public Key Encryption

Trusting the person that we're talking to requires two things: a unique way to represent the message to make sure it wasn't forged, and a way to verify the person who sent the message. The first part - representing messages in a unique way - can be solved with something called a message hash.

This is how public key cryptography can be used to verify the sender using a message signature.

The widget : verifying signatures



Meet by the basketball courts after school

Original Message Hash

6f45cb2158c58d866b9139b14fe608a3

Encrypted Message Signature

5aa912791fe5ba904edb5518f1bde2c7

Which public key do you want to try?

https://studio.code.org/s/blockchain-2023/lessons/2/levels/1?no_redirect=1

Several people have sent messages to the group, but we're not sure who sent which message! Luckily, each message was **signed** with someone's private key. To figure out who sent the message, we can use the public keys to verify the signature and determine who sent the message. This involves de-crypting the message signature to see if it matches the original message - if it does, then we know who was the authentic author of the message!

Do This

- Use the widget on the left to view the messages. You can use the orange arrows at the top to scroll between messages. There are four messages in total

- Choose a public key from the table below to try and decrypt the message signature
  - If the decrypted signature matches the original message: you've found the sender!

- ○ If not, then try another person's public key
- Repeat this process until all messages have been verified!

Use the widget on Code Studio to fill in the table below with the correct sender of each message

Message	Sender
Meet by the basketball courts after school	
Let’s hang out this weekend	
I brought some empanadas to share at lunch	
Someone told me Zoey is the coolest person in school	

4- Blockchain and Bitcoin

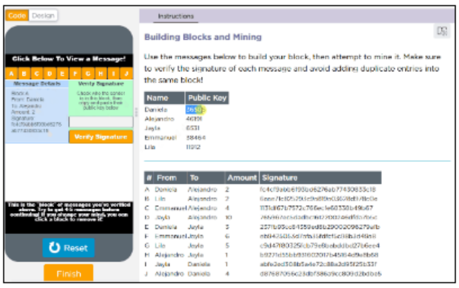
Using encryption is important when trust can be an issue - for example, sending a secret message and not wanting someone to eavesdrop on it. Another situation where trust can be an issue is with money and finances - how can two people exchange goods without needing to trust each other? This is a problem that the Blockchain and Bitcoin have been able to solve

Blockchain technology helps solve the problem of exchanging money without relying on a shared sense of trust - instead, people trust the underlying technology: encryption. However, there is still the need to verify the transactions and add those transactions to the blockchain. This is what the blockchain miners do. Let’s see if we can simulate what it would be like to be a miner on the blockchain.

The widget : mining blocks

https://studio.code.org/s/blockchain-2023/lessons/2/levels/2?no_redirect=1

Widget



Block A
From: Daniela
To: Alejandro
Amount: 2
Signature: fc4cf9abb6f93bd6276ab77430833c18

Check who the sender is in this block, then copy and paste their public key below

This is the "block" of messages you've verified above. Try to get 4-5 messages before continuing! If you change your mind, you can click a block to remove it!

Building Blocks and Mining

Use the messages below to build your block, then attempt to mine it. Make sure to verify the signature of each message and avoid adding duplicate entries into the same block!

Name	Public Key
Daniela	26505
Alejandro	46191
Jayla	6531
Emmanuel	38464
Lila	11212

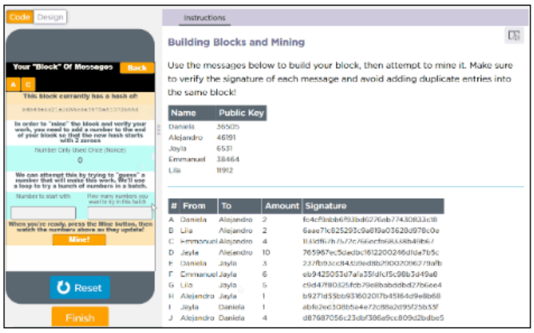
#	From	To	Amount	Signature
A	Daniela	Alejandro	2	fc4cf9abb6f93bd6276ab77430833c18
B	Lila	Alejandro	2	[illegible]
C	Emmanuel	Alejandro	4	1131d867b7572c766ec1e60330b49b67
D	Jayla	Alejandro	10	[illegible]
E	Daniela	Jayla	3	257fb93cc84159ed8b29002096279afb
F	Emmanuel	Jayla	6	[illegible]
G	Lila	Jayla	5	c9d47f803325fcb79e6bebddbd27b6ee4
H	Alejandro	Jayla	1	b9271d55bb931602017b4584d9e8b68
I	Jayla	Daniela	1	abfe3ed508b5a4e72c88a3d95f25b33f
J	Alejandro	Daniela	4	d87687056c23dbf386c9cc809d2bdbe6

Modeling Notes

- Click on each of the buttons to load a message. Each message represents a bitcoin transaction.
- Identify the sender of the message and find their public key in the table. Copy and paste their public key into the widget to verify the signature
- If the signature matches: you can add that message to your “block” by clicking the “Add To Block” button
- If the signatures don’t match: you can ignore that message since it’s a fraudulent message.
- As a class, work together to add 3-5 blocks, then press the Next Screen button.

Trying to find the correct nonce can only be done with guessing and trying lots of combinations, which is what makes this a proof of work. Let's look at how we can do this in the widget.

Widget



This block currantly has a hash of:

[illegible]

In order to "mine" the block and verify your work, you need to add a number to the end of your block so that the new hash starts with 2 zeroes

Number Only Used Once (Nonce)

0

We can attempt this by trying to "guess" a number that will make this work. We'll use a loop to try a bunch of numbers in a batch.

Number to start with

How many numbers you want to try in this batch

When you're ready, press the Mine button, then watch the numbers above as they update!

Building Blocks and Mining

Use the messages below to build your block, then attempt to mine it. Make sure to verify the signature of each message and avoid adding duplicate entries into the same block!

Name	Public Key
Daniela	36505
Alejandro	46191
Jayla	6531
Emmanuel	38464
Lila	11912

#	From	To	Amount	Signature
A	Daniela	Alejandro	2	fc4cf9bbb6f93bd6276ab77430833c18
B	Lila	Alejandro	2	6aae71c825293c9a819a03628d978c0e
C	Emmanuel	Alejandro	4	113dff67b7572c766ecfa68338b48b67
D	Jayla	Alejandro	10	765967ec5dadbc1612200246d1da7b5c
E	Daniela	Jayla	3	237fb93cc8435d9ed8b2900208627 9afb
F	Emmanuel	Jayla	6	eb9425053d7afa35ldfcl5c98b3d49a8
G	Lila	Jayla	5	c9d47f80325fcb79e8babddbd27b6ee4
H	Alejandro	Jayla	1	b9271d55bb931602017b45164d9e8b68
I	Jayla	Daniela	1	abfe2ed308b5a4e72c88a2d95f25b53f
J	Alejandro	Daniela	4	d87687056c23dbf386a9cc809d2bdbe5

Modeling Notes

- When the level loads, it will automatically reveal the steps to begin mining and completing a proof of work
- Choose a starting number to test for your nonce. You can ask students to suggest this number
- Choose how many numbers to try. You can also ask students to suggest this number.
- Press the Mine button and see if a match is found!
- If no match is found, choose a new starting number or a new range to test and try again!

Blockchain Scenario #1

Use the widget on Code Studio to record your work building a block on this particular blockchain.

Which messages were valid?	**Which messages were invalid?**
Which messages did you include in your block?	**What was the nonce you found**

Since the transactions are public, we can see how these people are trading money. Does it look like this scenario has a pattern? If so, what story can you tell about that scenario amongst this group of friends?

Blockchain Scenario #2

Use the widget on Code Studio to record your work building a block on this particular blockchain.

Which messages were valid?	**Which messages were invalid?**
Which messages did you include in your block?	**What was the nonce you found**

Since the transactions are public, we can see how these people are trading money. Does it look like this scenario has a pattern? If so, what story can you tell about that scenario amongst this group of friends?

Blockchain Scenario #3

Use the widget on Code Studio to record your work building a block on this particular blockchain.

Which messages were valid?	**Which messages were invalid?**
Which messages did you include in your block?	**What was the nonce you found**

Since the transactions are public, we can see how these people are trading money. Does it look like this scenario has a pattern? If so, what story can you tell about that scenario amongst this group of friends?

Blockchain Scenario #4

Use the widget on Code Studio to record your work building a block on this particular blockchain.

Which messages were valid?	**Which messages were invalid?**
Which messages did you include in your block?	**What was the nonce you found**

Since the transactions are public, we can see how these people are trading money. Does it look like this scenario has a pattern? If so, what story can you tell about that scenario amongst this group of friends?