CSE 469 FALL 2023

Group Project: Blockchain Chain of Custody

Aditya Gheewala
CySA+, Security+

agheewal@asu.edu
Discord: Aditya (dav1c11)

Chain of Custody (Evidence)

- When you are given an original copy of media to deal with, you need to document the handling:
    - Where it was stored
    - Who had access to it and when
    - What was done to it
- Shows that the integrity of evidence/data was preserved and not open to compromise.
- Route the evidence takes from the time you find it until the case is closed or goes to court.

Traditional
Chain of Custody Form

Print Form

PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

APLCS, LLC (http://www.aplcs.com)

Case Name:		**Reason Obtained:**	
Case Number:			
Item Number:	**Evidence Type / Manufacturer:**	**Model Number:**	**Serial Number:**
Content Owner / Title:	**Content Description:**		
Content Owner Contact Information:			
Forensic Agent:	**Creation Method:**	**HASH Value:**	**Creation Date/Time:**
Forensic Agent Contact Information:			

CHAIN OF CUSTODY

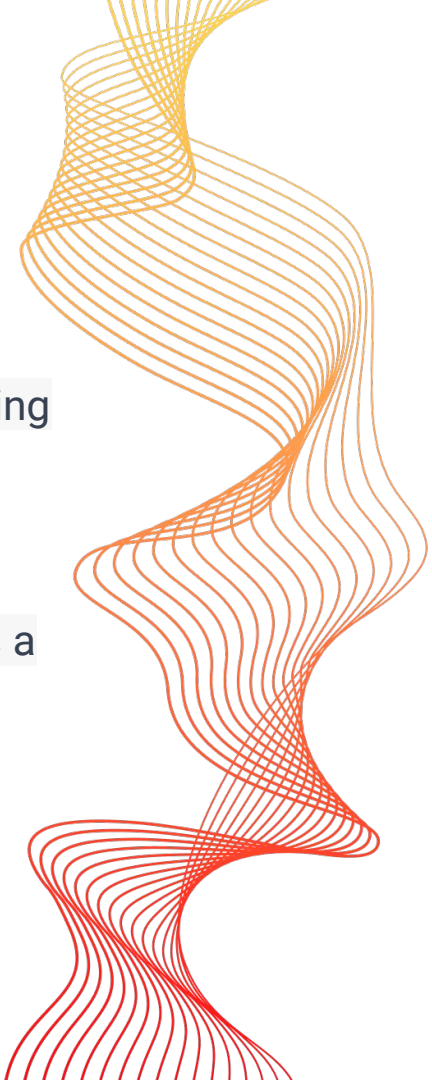
Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	

Item Number: _____

Page: 1 of _____

Challenges of Digital Evidence

- **Ease of Alteration**: Digital evidence can be easily altered, making integrity preservation even more critical.
- **Chain of Custody Trail**: Tracking digital evidence through its lifecycle is complex, given its intangible nature.
- **Authentication**: Ensuring the authenticity of digital evidence is a challenge.

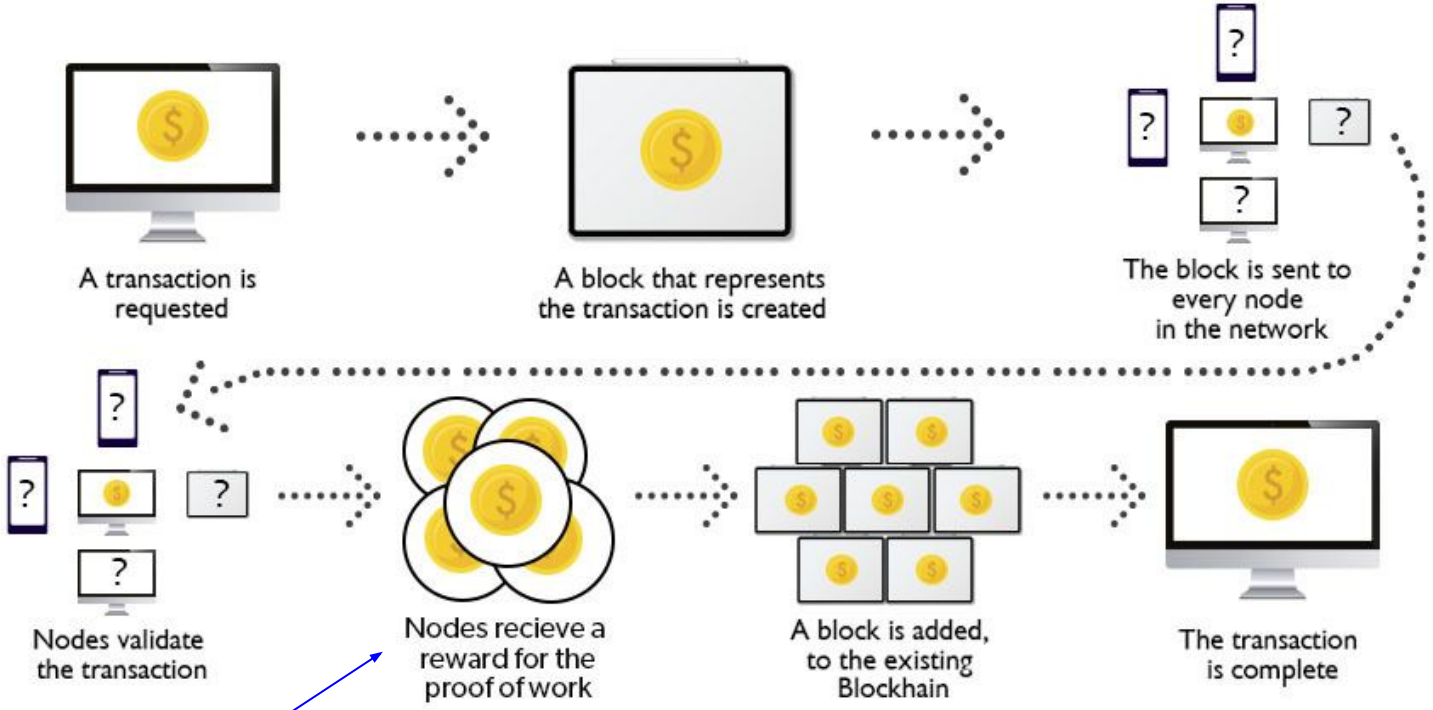


Blockchain

Key Characteristics:

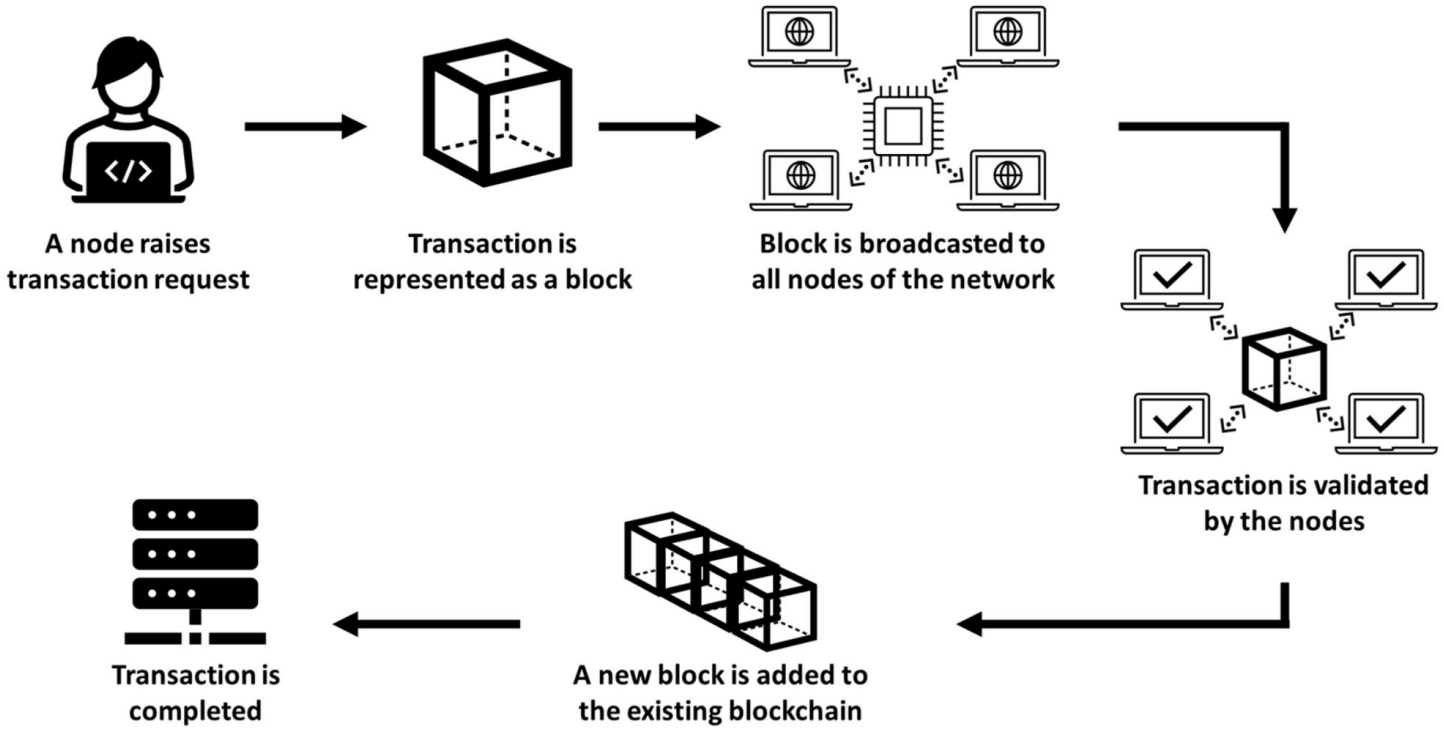
- **Decentralization**
  - no central authority or intermediary
  - All participants (nodes) in the network have equal authority and control
- **Immutability**
  - Once data is recorded in a block, it becomes extremely difficult to alter or delete
- **Transparency**
  - Every participant in the network can view the entire blockchain.

How Blockchain Works?

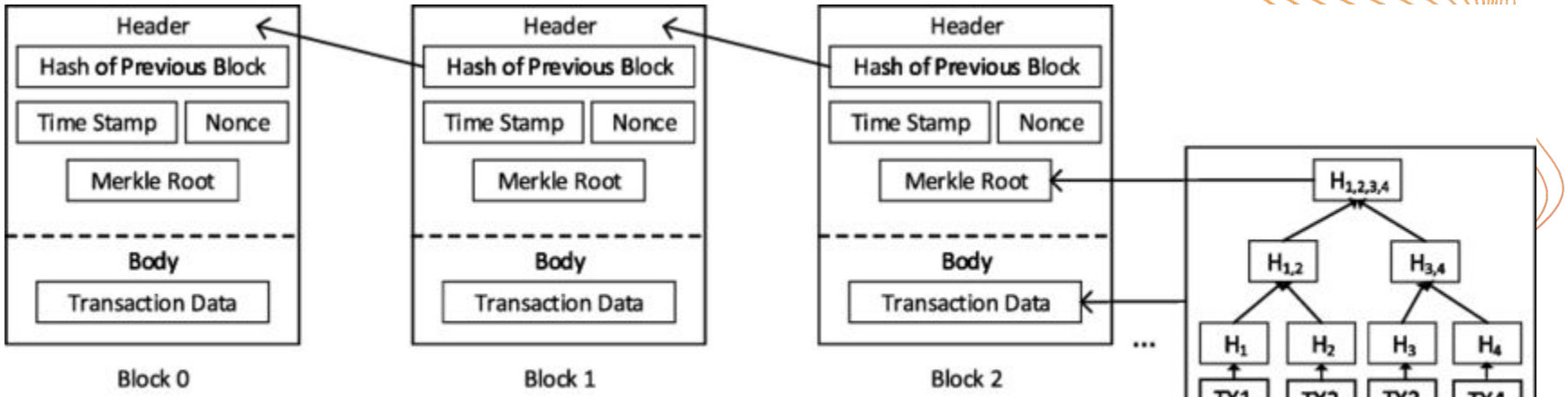


You need to indicate that his flow is an example in cryptocurrency.

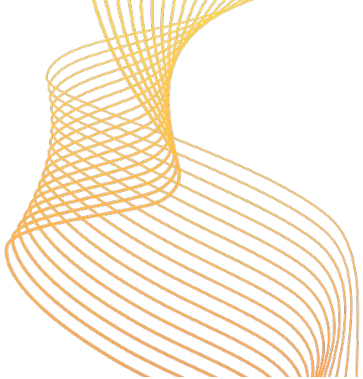
How Blockchain Works?



Block Structure



Genesis Block and Integrity Check

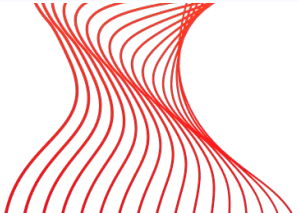


- Timestamp: 1231006505
- Difficulty: 4
- Nonce: 0
- Previous hash: 0
- Merkle root: 4a5e1e4d2c7f9a67962e0ea1f61deb649f6bc3f4cef387fe9b263ae2c0f86e56
- Transaction data:

```
Message: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"
Value: 50 BTC
Recipient: Satoshi Nakamoto
```

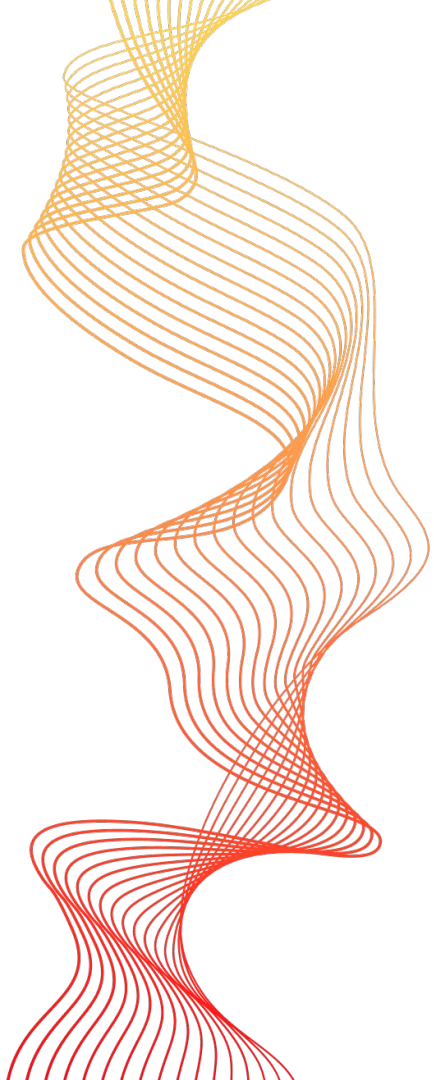
- Timestamp: 1434971280
- Difficulty: 3
- Nonce: 2089236893
- Previous hash: 0
- Merkle root: 0x6fe28c0ab353a9423258c2c6fce7525942b67d12271
- Transaction data:

```
Message: "The first block on the Ethereum blockchain"
Value: 5 ETH
Recipient: Vitalik Buterin
```



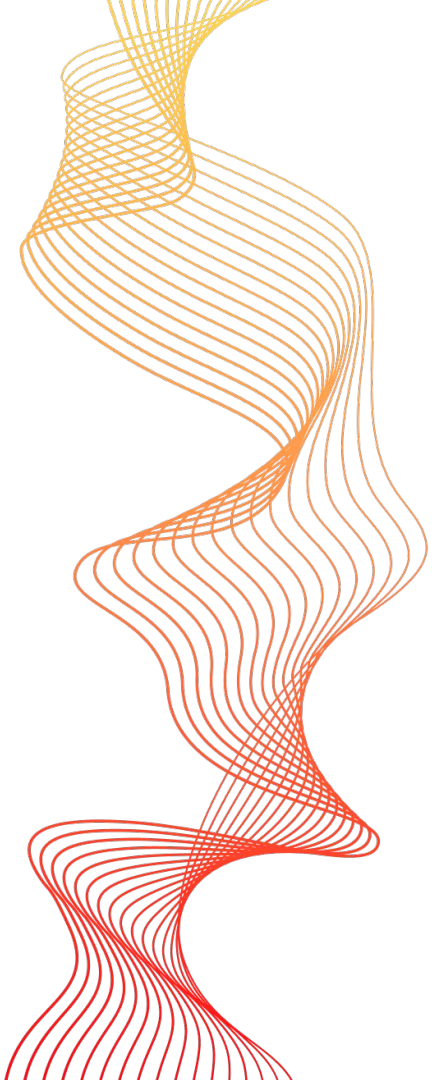
Blockchain Demo

https://blockchaindemo.io/



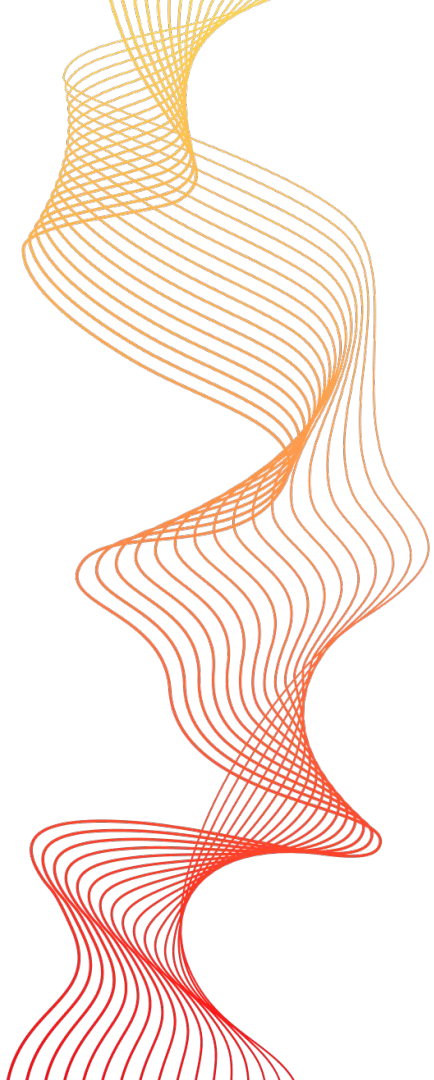
Project Overview

- Write a program that will be a digital equivalent of a chain of custody form.
- Each entry in the form will be stored in a blockchain of your own creation.



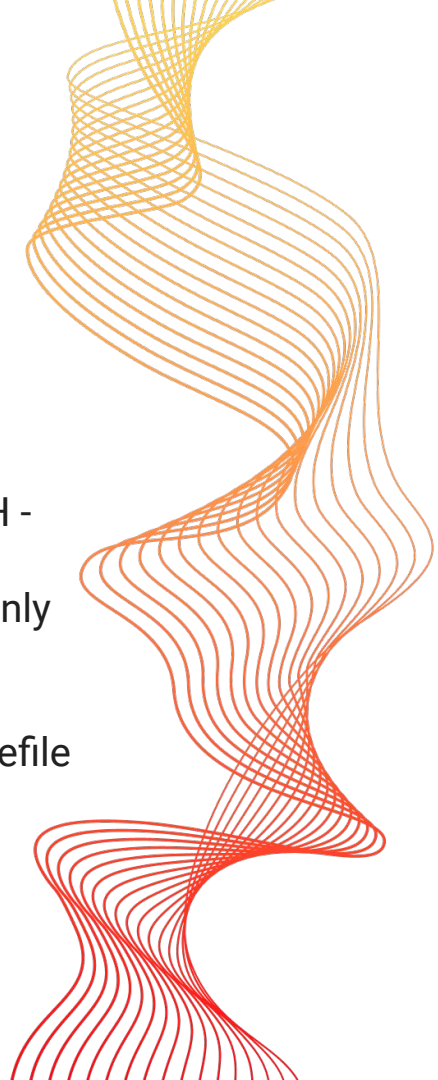
Demo session

1. Programming Language based
2. Etherium
3. Hyperledger



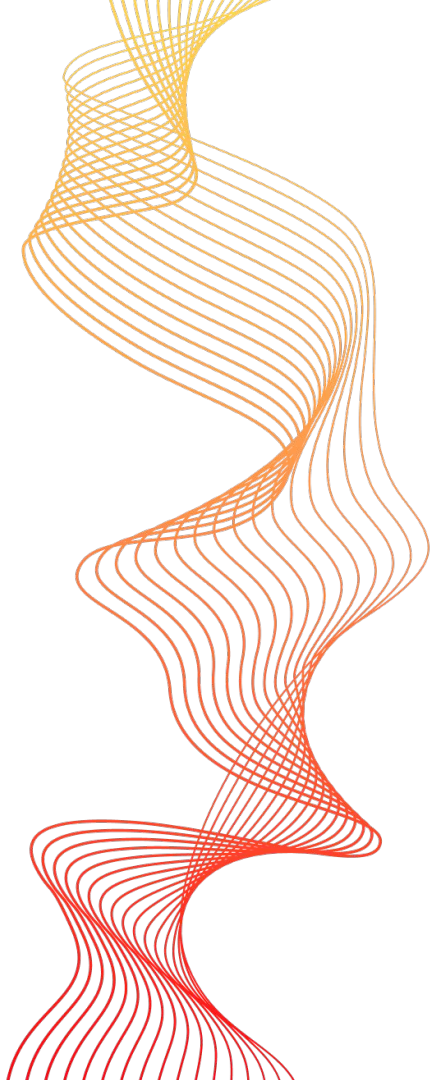
FAQs

- Calling the program - “./bchoc ….”
- Options - using the command-line arguments
- Where to save the blockchain (blocks/data) - BCHOC_FILE_PATH - this env variable will have the filepath
- Edge cases and condition checks - recommended but required only those mentioned in the guidelines document
- Installing extra packages - Add a “packages” file (no extension)
  - For python libraries, add the installation commands in makefile
- Slides, videos and report
- Output formatting issues



FAQs

- OS preference
- Data Structure



Project Guidelines

https://docs.google.com/document/d/1BNbntxyTXiSGeRfeZylozLNn_Nb9NY0Xer9PIuPfQ3s/edit?usp=sharing