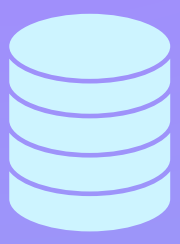
BLOCKCHAIN

THE FUTURE OF SECURITY

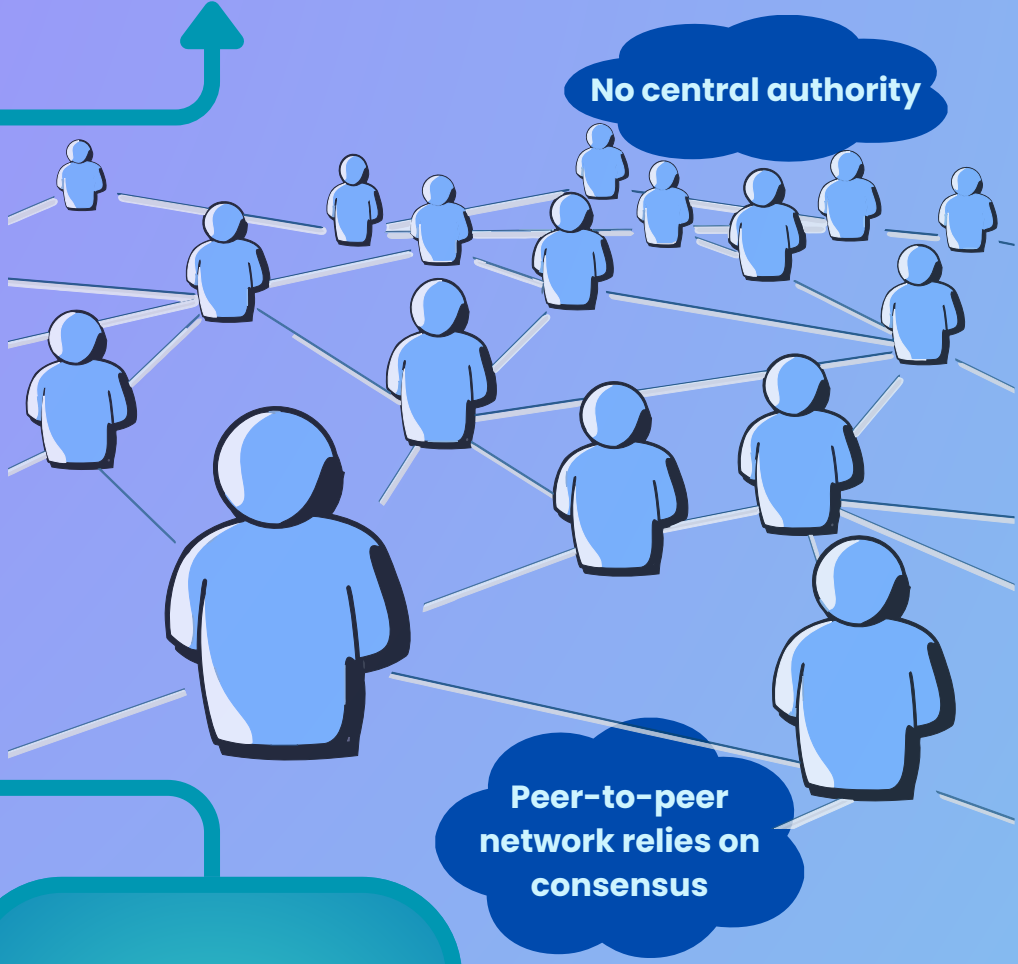
Anyone can access the blockchain and be sure they are seeing the **same chain of events** as everyone else



Central databases require **trust**

Blockchain eliminates the question, "Who owns the database?"

As long as 51% of the blockchain network is honest, malicious nodes cannot undermine its integrity



Cryptocurrencies are built into blockchain operation, but blockchain applications can do much more than simple transactions

By digitally signing each transaction, no one can deny actions they've taken in the past

Smart contracts are collections of functions, written in **Solidity**, that form the basis for **decentralised apps** (DApps)

Digital signatures use encryption techniques to verify each transaction's sender

Hash functions create a "fingerprint" of data. Any size of input creates a fixed-size, random-looking output

All of the computers on Earth, working for the age of the universe, could not "undo" a 112-bit hash function

This research was supported by the Valerie Kuehne Undergraduate Research Awards, University of Victoria

I built **SecureBid**, an auction **DApp**, using

- Solidity
- Web3.js
- React
- Next.js

Check it out on GitHub!

The smart contract acts as the auctioneer and bidders **commit** to and **seal** their bids using a hash function

Blockchain can be applied anywhere we need a reliable history of events

- Vehicle passports
- Supply chain
- Money transfer
- Internet of Things
- Healthcare

By **Zoë van de Vegte**
Electrical and Computer Engineering
Supervised by **Dr. Riham AlTawy**

1 Sept. 2024

University of Victoria