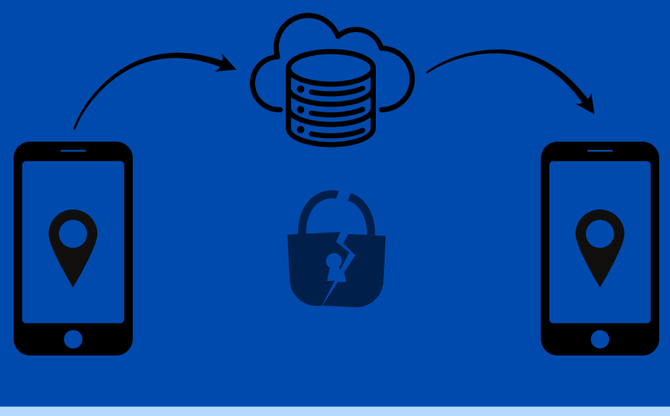
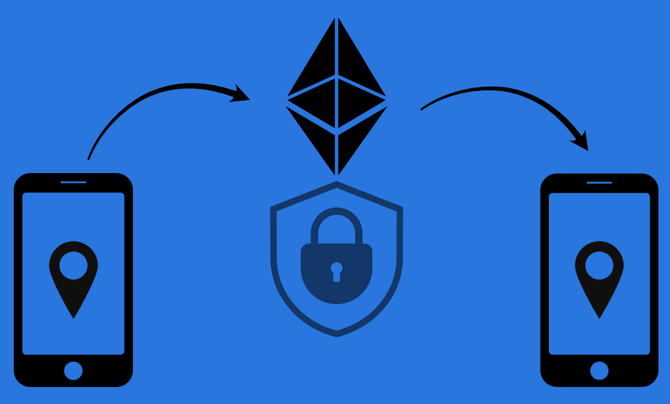
Decentralized Location Sharing Using Blockchain

Rylan Peebles - Electrical and Computer Engineering
Supervised by Dr. Riham AlTawy

The Issue with Conventional Location Sharing

When you share your location with a friend or family member using your smartphone, that location data is sent to a cloud server hosted by a large tech company like Apple or Google, and is read from the cloud server by the recipient's device. This gives tech companies control over your private information.



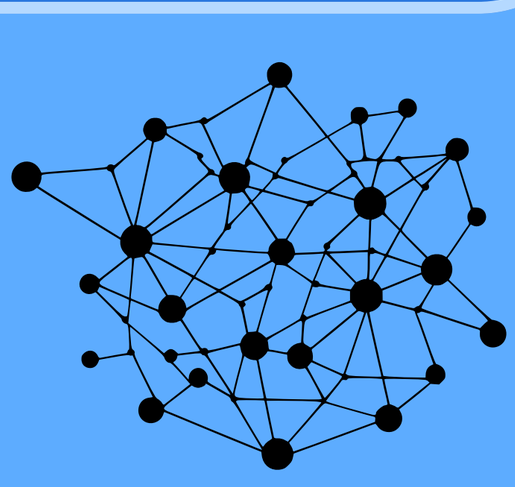


Taking a Decentralized Approach

This issue can be solved by leveraging the security, immutability, and decentralized nature of blockchain technology. Instead of using a cloud server, location coordinates can be encrypted and uploaded to the Ethereum blockchain, where they are visible to everyone, but can only be modified by the sender or decrypted by the recipient.

How Blockchain Works

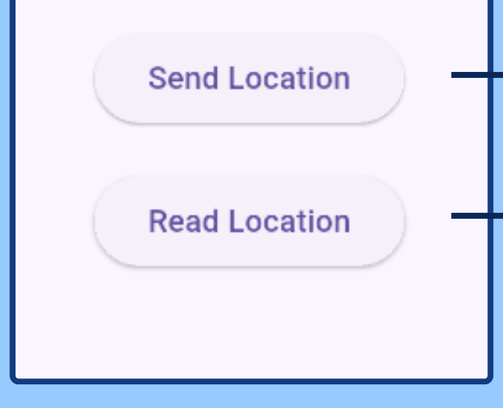
Blockchain was originally invented as a decentralized currency, but the underlying technology has broader applications. Instead of relying on large computers controlled by one company (i.e., cloud servers), blockchain uses many independent computers connected in a peer-to-peer network to verify the info contained in the blockchain and continue building it (e.g., Bitcoin, Ethereum). This ensures no central authority has control over the blockchain; however, blockchains require more computing power to operate, so they charge fees for use, making them a more expensive alternative to centralized computing.



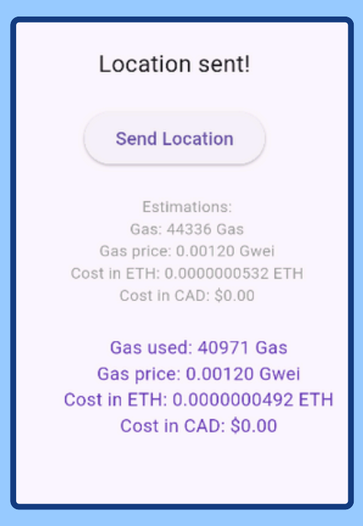
Peer-to-Peer Network

My Design

I developed a mobile app that encrypts coordinates and uploads them, or decrypts them and displays them on a map. This solution eliminates the need for a trusted central authority.

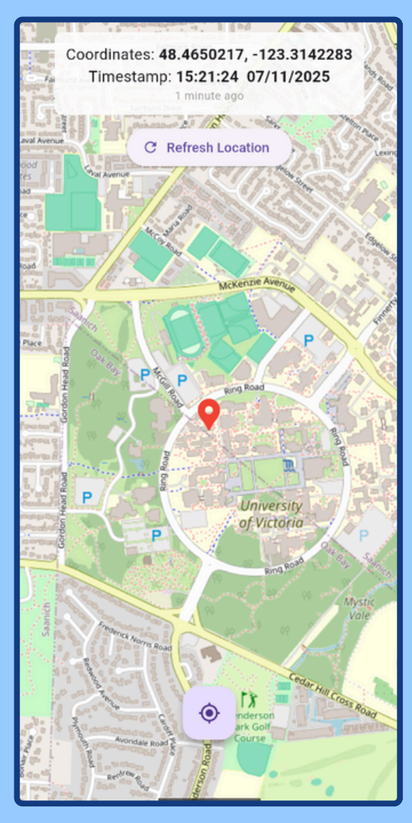


Home page lets you connect your wallet and send or read location. An Ethereum wallet needs to be connected to interact with the blockchain.



Location sending page displays blockchain network fee estimations before sending, and actual values once sent.

When the location is read, a pin is shown on an interactive map. It also shows the time the location was uploaded and how long has passed since. Reading data off the blockchain incurs no fees.



Flutter
Dart

The mobile app was developed on an emulator in Android Studio, using the Flutter software development kit and Dart Programming Language.

Encryption was achieved using Advanced Encryption Standard (AES).

AES

Conclusion

This proof of concept demonstrates that further development of a more widely usable location-sharing DApp is possible. Such a DApp would cost more than conventional location sharing technologies, but would require no trusted intermediary to function; it would exist independently of the large tech companies that control this service today.

Increased cost

Increased security

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

University of Victoria