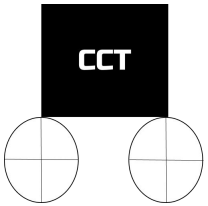
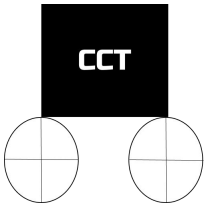


CarConTracks: A Peer-to-Peer Car Rental DApp

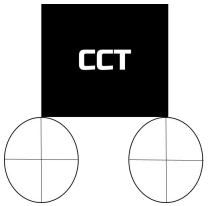
Negar Yassaie, Sara Gargoum, Mateusz Faltyn

Outline



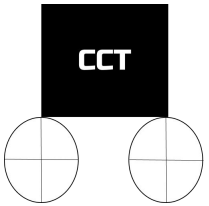
1. Introduction
2. Objective
3. Related Work
4. Traditional Apps vs DApps
5. Design
6. Security
7. Demo
8. Future Work

Introduction



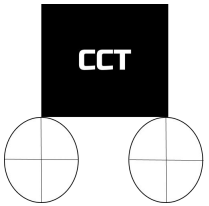
- As COVID-19 pandemic restrictions continue to lift across Canada and much of the rest of the world, the commuting landscape looks very different than it had before March 2020.
- The overall trend is clear: **individuals want to increasingly rent, not buy, vehicles.**
    - Global vehicle sales have been decreasing since their peak in 2016 with a decrease of around 13.8% between 2019 and 2022.
    - Additionally, global vehicle production has fallen from around 97 million per year in 2017 to 78 million per year in 2020.

Objective



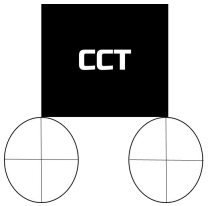
- To create a peer-to-peer car rental decentralized application entitled CarConTracks that:
  - is an Ethereum-based DApp that…
  - allows individuals with the appropriate legal qualifications (i.e., age and driver’s license)…
  - to rent or loan a car for a specific duration of time.

Related Work



- **Modo** is a car rental service that allows a user to pick up a car, rent it for a specific duration time, and return it to the same location as where it was picked up.
- **Evo** allows a user to rent a car for a specific duration and drop it off at any location listed on the app.
- To our knowledge, no DApp currently exists that fulfills the needs of car renters and rentees.

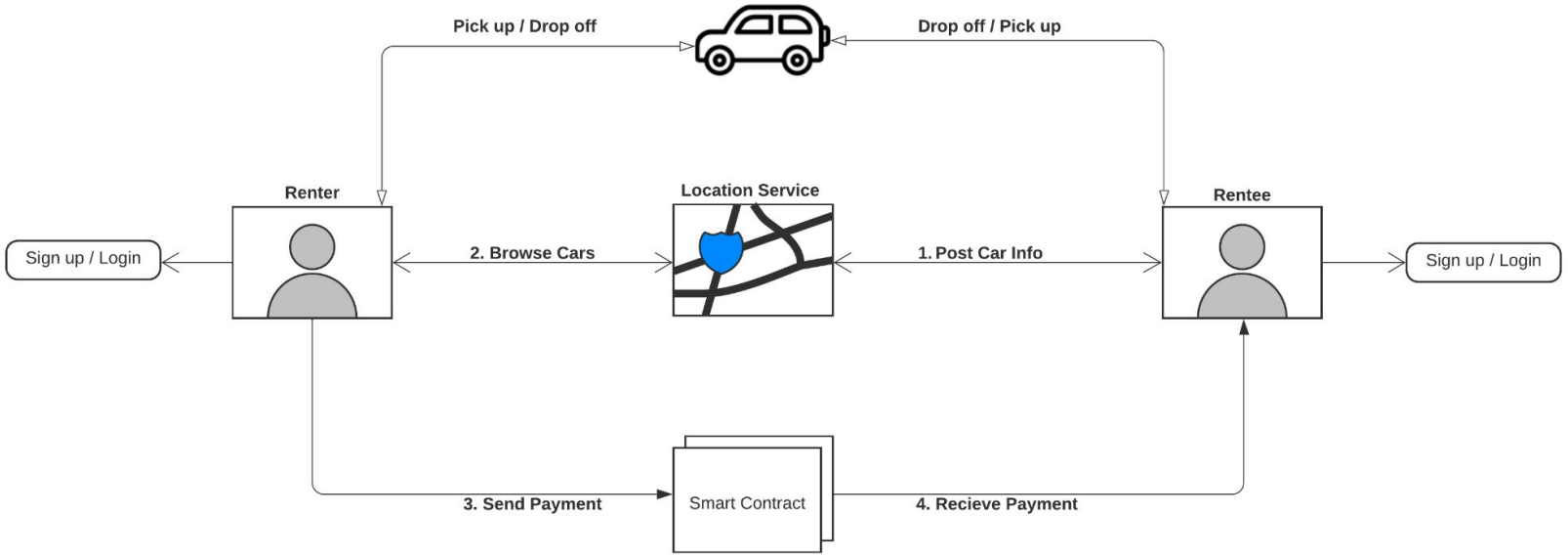
Traditional Apps vs DApps



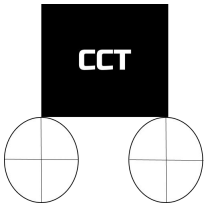
- Traditional apps are vulnerable to data tempering.
- Traditional apps are opaque.
- Traditional apps have a central point of failure.

- DApps are more secure and their data is immutable.
- DApps have better transparency for users.
- DApps are open source.

Design - Architecture



Design - Smart Contract



User Functions:

- Sign up
- Login
- Logout

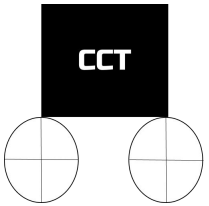
Rentee Functions:

- Add car

Renter Functions:

- Create rental
- Confirm rental
- Cancel rental
- Return car

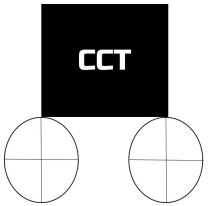
Smart Contract Security - Slither



- Slither by Trail of Bits
- Solidity static analysis framework written in Python 3

```
Compiled with solc
Number of lines: 288 (+ 0 in dependencies, + 0 in tests)
Number of assembly lines: 0
Number of contracts: 1 (+ 0 in dependencies, + 0 tests)

Number of optimization issues: 20
Number of informational issues: 33
Number of low issues: 0
Number of medium issues: 2
Number of high issues: 1

+-----------+-------------+------+------------+--------------+-------------+
|    Name   | # functions | ERCS | ERC20 info | Complex code |   Features  |
+-----------+-------------+------+------------+--------------+-------------+
| CarRental |      23     |      |            |      No      | Receive ETH |
|           |             |      |            |              |   Send ETH  |
+-----------+-------------+------+------------+--------------+-------------+
```

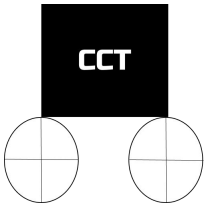
Smart Contract Security - Echidna



- Echidna by Trail of Bits
- Haskell program designed for fuzzing/property-based testing of Ethereum smart contracts

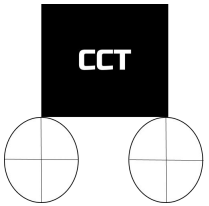
```
~/Desktop (174.795s)
echidna-test CarRental-fuzz.sol --test-mode assertion

Analyzing contract: /Users/mateuszfaltyn/Desktop/CarRental-fuzz.sol:CarRental
getBalanceofSC():  passed! 🎉
confirmRental():  passed! 🎉
SignUp(address,string,string):  passed! 🎉
returnCar(uint256):  passed! 🎉
getorderReturn():  passed! 🎉
createRental(string,uint256,uint256,uint256): failed!💥
  Call sequence:
    addCar("\NUL","\NUL")
    createRental("\NUL",643985938241415395878581184108060,1,1) Value: 0x1647d1068d15452

Event sequence: Panic(1)
balances(address):  passed! 🎉
getcustomerName():  passed! 🎉
getcarID(uint256):  passed! 🎉
getorderConfirmation():  passed! 🎉
getorderValidity():  passed! 🎉
cancelRental():  passed! 🎉
totalCarNum():  passed! 🎉
rentals(address):  passed! 🎉
addCar(string,string):  passed! 🎉
getBalanceofOwner():  passed! 🎉
getcarAvailability(uint256):  passed! 🎉
price():  passed! 🎉
Login(address,string):  passed! 🎉
getcarLocation(uint256):  passed! 🎉
logout(address):  passed! 🎉
getcustomerAge():  passed! 🎉
getownerName(uint256):  passed! 🎉
getlicenseID():  passed! 🎉
cars(uint256):  passed! 🎉
AssertionFailed(..):  passed! 🎉

Unique instructions: 6053
Unique codehashes: 1
Corpus size: 31
Seed: 4338789481903262629
```

Demo



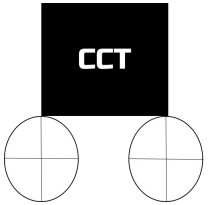
- We will now show you a demo of our project!

Future Work



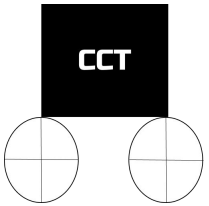
- Google Maps interface via the Google Maps API to display the nearest available car.
- Communication platform between renters and rentees.
- User compliance features to the DApp (KYC).
- Smart contract security improvements (Fuzzing via Echidna).
- Release Car Rental (CARR) ERC-20 Token.

References



- [1] M. Garaus and C. Garaus, “The Impact of the Covid-19 Pandemic on Consumers' Intention to Use Shared-Mobility Services in German Cities”. Front. Psychol. 12:646593. doi: 10.3389/fpsyg.2021.646593
- [2] K. M. Kiran Raj and K. G. Nandha Kumar, “Impact of Covid-19 Pandemic in the Automobile Industry: A Case Study”, International Journal of Case Studies in Business, IT, and Education (IJCSBE), vol. 5, no. 1, pp. 36–49, Feb. 2021, doi: 10.5281/zenodo.4505772.
- [3] "Topic: Automotive industry worldwide", Statista, 2022. [Online].
- [4] "Modo | Carsharing made easy", Modo.coop, 2022. [Online]. Available: https://modo.coop/. [Accessed: 20- Mar- 2022].
- [5] "Car Sharing Vancouver", Evo, 2022. [Online]. Available: https://evo.ca/. [Accessed: 20- Mar- 2022].
- [6] F. Casino, T. Dasaklis and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues", Telematics and Informatics, vol. 36, pp. 55-81, 2019. Available: 10.1016/j.tele.2018.11.006.
- [7] "Trail of Bits", Trailofbits.com, 2022. [Online]. Available: https://www.trailofbits.com/. [Accessed: 20- Mar- 2022].
- [8] V. Buterin, "A next-generation smart contract and decentralized application platform", Whitepaper, 2014
- [9] W. Bolt and M. van Oordt, “On the Value of Virtual Currencies”, Tech, Working Paper, 2016.
- [10] Brave Software. "Basic Attention Token (BAT): Blockchain-Based Digital Advertising", Whitepaper, 2021.

Questions?



- Thank you for listening!
- Check out the app at https://github.com/mattfaltyn/CarConTracksV1