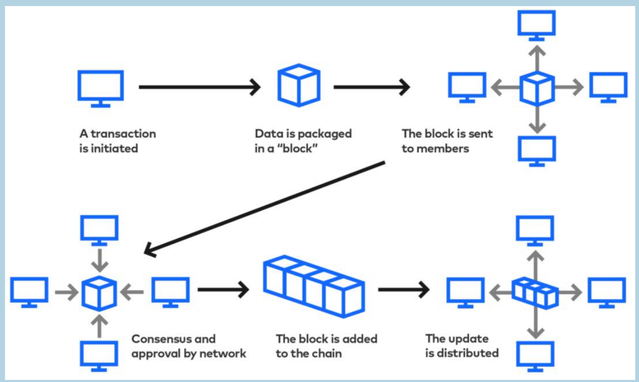
A lightweight and democratic Blockchain consensus over mobile device

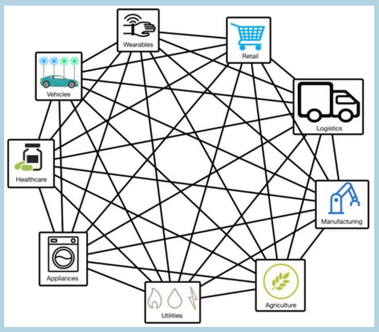
Project member： Zhuang Zhan, Zou Ruotong, Pan Taiyang, Yun Musheng Adviser: Song Xuan
Department of Computer Science and Engineering, Southern University of Science and Technology

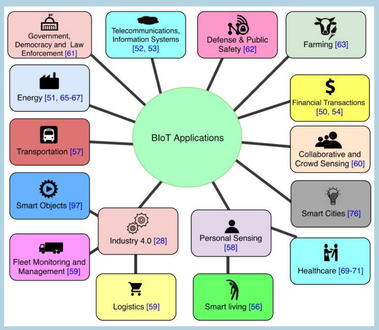
Introduction

Background

Blockchain is actually a distributed storage technology, a database that is jointly participated and maintained by many network nodes, based on P2P network technology.







Consensus mechanism

The mainstream

POW:
Resource: Power x Time

POS:
CoinAge: Quantity x Days

DPOS:
Democratic vote

AuxPOW:
Auxiliary blockchain

State-of-the-art

Time	Technology	Detail
2019.01	Algorand	Based on verifiable random function
2019.06	PoET	Based on lottery consensus
2019.08	PoRX	Based on reputation proof
2020.03	PoBT	Based on block and trade
2020.06	PoWP	Based on the presence of witnesses
2020.09	PoQF	Based on VANET and edge computing
2020.11	PoEWAL	Based on timed work and lucky values
2020.11	Blockene	Blockchain architecture on mobile phone

Problems

- Waste of computing resources and long settlement cycle.
- The computing power resources are centralized.
- Lack of popularity and and fairness.
- Blockchain mining equipment demand problem.
- Blockchain does not play its due value.

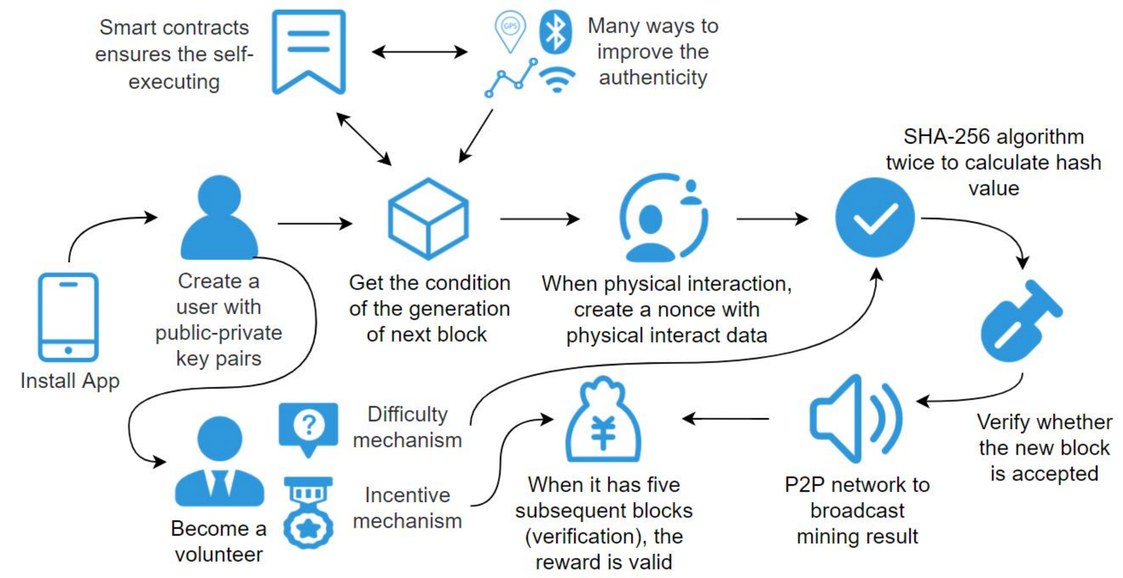
Advantages

Decentralization
Openness
Immutability
Traceability
Anonymity

Abstract: We propose a universal and lightweight proof of physics interaction (PoPI) consensus mechanism and its integration framework based on a mobile device app. Also, we propose the incentive mechanism and difficulty mechanism based on a volunteer mechanism to guaranteed the robustness. This is the prototype of the theory of mobilecoin.

Methodology

System Framework



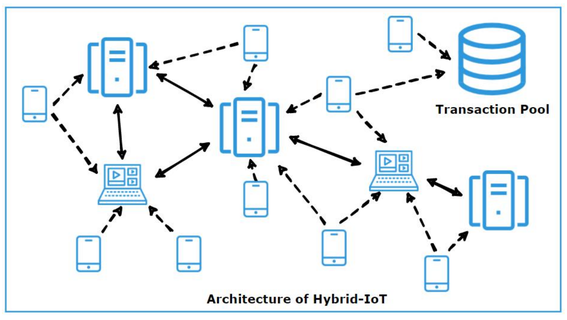
Physical Interactive Data

Finiteness:
Related to time, space and number of people.

Dependability:
GPS, Bluetooth, WIFI and other channel detection.

Randomness:
Generates random numbers that cannot be forged.

System Architecture



Incentive

Production Reward:
Rewards for solving hashing difficulties.

Package Reward:
Rewards for packaging transactions.

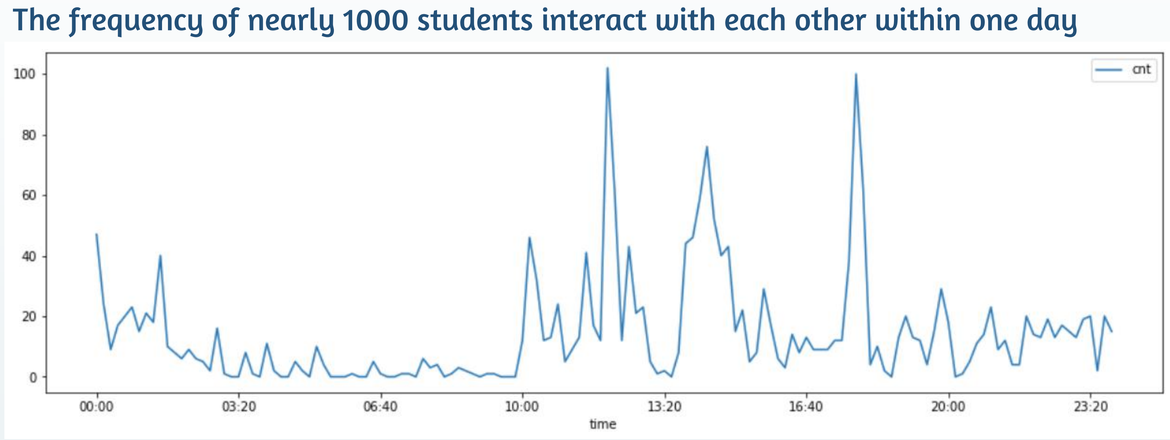
Volunteer Reward:
Rewards for being a volunteer baseline.

Key Issues Discussion

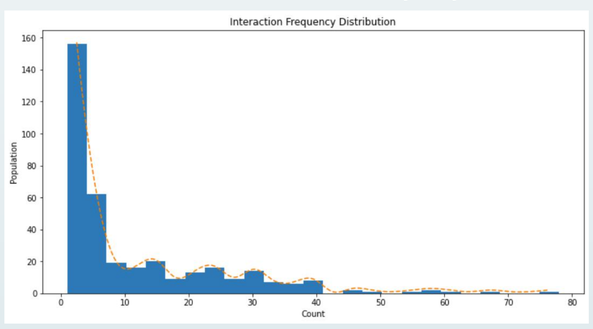
Forking Attack: The physical interaction data used by Mobilecoin is limited, and its total amount is positively correlated with the total number of active users. So in this system, the computing power is dispersed, which effectively prevents the forking attack.
Forging Data: The physical interaction data used by Mobilecoin is real, furthermore, it can be verified in multiple ways such as GPS, Bluetooth, history trajectory data and other sensors. We can also establish a self-executing smart contract in the mining process as a random item generation condition.
Difficulty Adjustment: We use the mainstream difficulty adjustment method combined with the volunteer mechanism. Volunteer users share data such as the number of interactions per time period to the central server as a benchmark.

Results

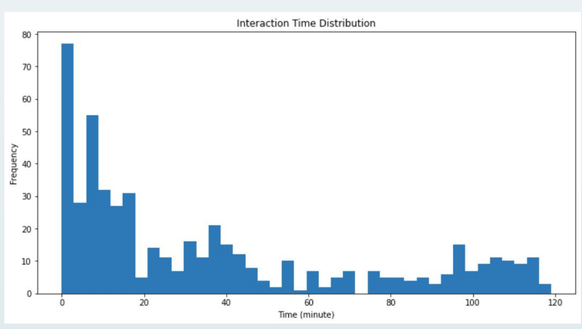
The frequency of nearly 1000 students interact with each other within one day



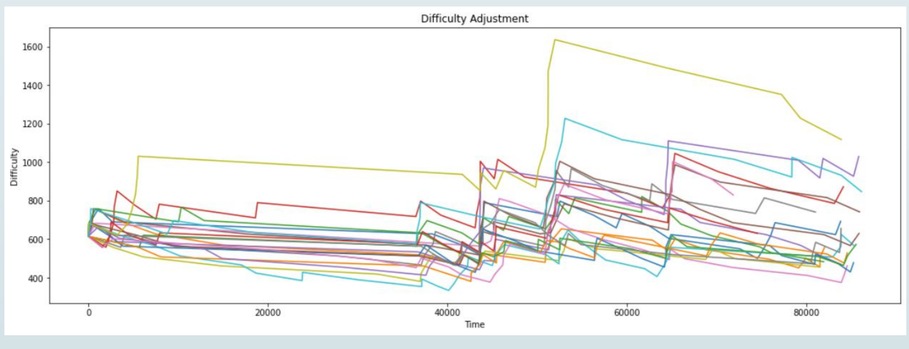
Interaction distribution over people

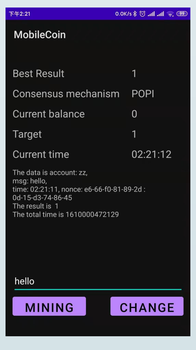


Interaction distribution over time



The changes of Mobilecoin difficulty in one day under test conditions





Conclusion

Contribution

- Fairness: Equal mining equipment
- Efficiency: Mobile device (Bluetooth, GPS, etc)
- Universal: Anyone can simply participate
- Perspectiveness: Internet of Things

Future

- Improve the ability of network development and mobile app development through reading and internship, then improve the project and launch mobilecoin.
- Enrich the theoretical knowledge and enhance the accuracy and robustness of the theoretical model (PoPI). And then we will complete two or three high-level papers.
- Complete larger tests, and determine the value of parameters according to the results.

Acknowledgements

We would first like to thank our supervisor, inspector and all the tutors in the SUSTech-UTokyo Joint Research Center on Super Smart City who guided us through the project and provided a lot of valuable advice. I would also like to thank the Department of Computer Science and Engineering for giving us this opportunity. Finally, we could not have completed this project without the ddls.

Reference

[1] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. Ieee Access , 6 , 32979-33001.
[2] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling.
[3] Nakamoto S, "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf[Online], 2008.
[4] Satija, S., Mehra, A., Singanamalla, S., Grover, K., Sivathanu, M., Chandran, N., ... & Lokam, S. (2020). Blockene: A High-throughput Blockchain Over Mobile Devices.
[5] "How blockchain will disrupt your industry", https://www.slalom.com/insights/how-blockchain-will-disrupt-your-industry[Online].