

Mobile Charger Billing System Using Lightweight Blockchain

Phebe John

Department of Computer Applications

College of Engineering Trivandrum

1st October 2018

Slides

1 Introduction

2 Blockchain

3 Architecture

4 Conclusion

5 Reference

Introduction

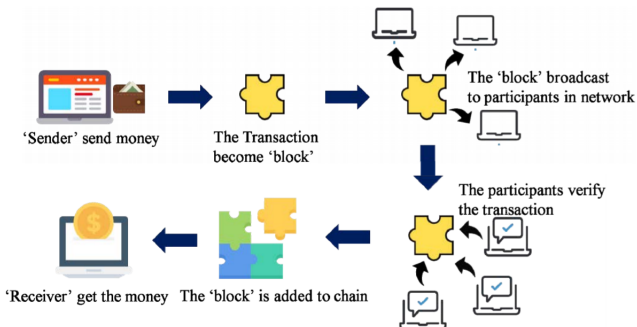
- Green transportation such as electric vehicles are emerging as an alternative to the traditional vehicles.
- They operate by using electric charging.
- The way to charge an electric car is to use a mobile charger or use a charging infrastructure.
- A billing system is required through which a user is billed who has charged the electric vehicle.
- It is a mobile charger billing system that utilizes Blockchain technology.

Blockchain

- Current online transaction rely on certain trusted institutions.
- These third party sources can be hacked, manipulated or compromised .
- The Blockchain technology to solve the problems.
- It explains electronic cash which is dealt in peer-to-peer network so that direct transactions can be made between the two parties without trading through a third trusted institution.
- A Blockchain is essentially a public ledger that is executed and shared between participants.



Online Transaction Using Blockchain

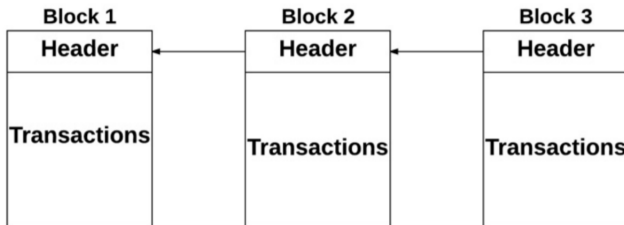


Blockchain Structure

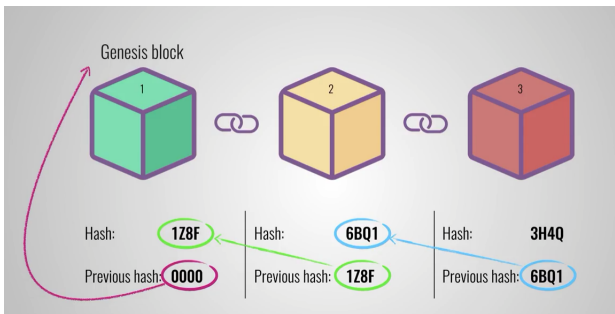
- Each Blocks constituting a Blockchain consist of a 'block header' and a 'block body'.
- The block header includes
 - Hash value of the previous block
 - Timestamp
 - Merkle Tree Root
- Each block is linked by a linked list method such as a chain.
- Block bodies may contain different values depending on its service.



Blockchain Structure



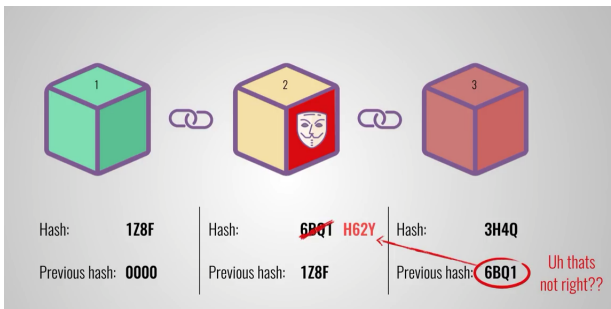
Blockchain Structure after Hashing



Modification of Data

- Here, I have a chain of three blocks.
- Each block has a hash and a hash of the previous block.
- So block 3 points to block 2 and block 2 points to the block 1.
- Now the block 1 is special. It is the Genesis block.
- Now if block 2 is tampered, it changes the hash of the block 2.
- Computers are very fast and they can calculate hash at a very high speed.

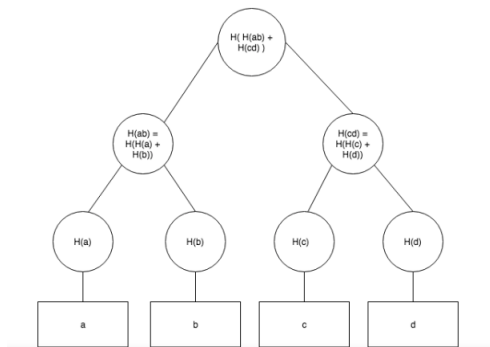
Modification of Data



Simplified Payment Verification - SPV

- Space and Power-constrained devices cannot maintain the full Blockchain.
- A simplified payment verification (SPV) is used to operate without the full Blockchain.
- SPV nodes download only the block header rather than the complete chain.
- Therefore, they do not know about the transactions.
- SPV node will establish a link between the transaction and the block that contains it, using a Merkle Path.

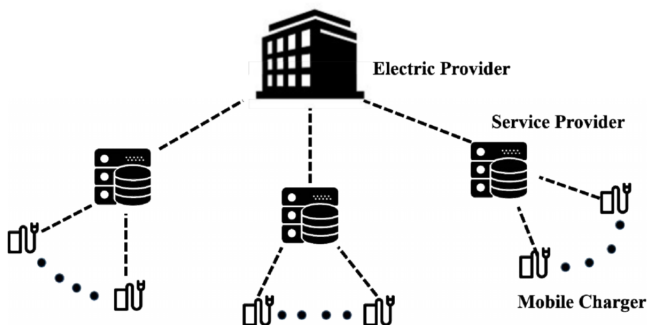
Merkle Path



System Architecture

- The system consists of a power supplier, a service provider, and a mobile charger.
- It is assumed that both the Service Provider and the mobile charger parent node are Full Block.
- The remaining mobile chargers utilize SPV.

System Architecture



Mobile charger packet information for billing

- It is assumed that each mobile charger knows the IP address of its own service provider.
- Each mobile charger can obtain the information of the current block and the neighboring node through the service provider.
- Table I shows the message type whereas the data types are specified in Table II.
- If certain mobile chargers are grouped together, they can be grouped by passing their groupid value to their service provider.

Message Type

Message	Description
Register	The mobile charger registers itself by transferring its 'idTag' to the Service Provider Server.
RegisterAck	Response message to 'Register'.
CheckAuth	If a new mobile charger is added, the Service Provider server forwards this message to the parent node of the group.
CheckAuthAck	Response message to 'CheckAuth'
Authorize	A mobile charger participating in a group requests permission to join the group by sending its idtag.
AuthorizeAck	Ack Response message to 'Authorize'

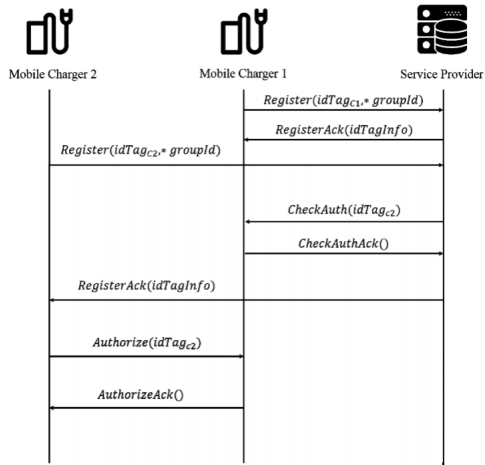


Data Type

Type	Description
idTag	Mobile Charger unique identifier
idTagInfo	It is delivered after registration. There are 'Interval', 'currentTime', 'status' fields.
Interval	Cycle to send 'ChargeProfile'
currentTime	The current time in the Service Provider. It is used to synchronize the mobile charger's internal clock
ChargeProfile	Consists of idtag and each charge history. Charging history includes start time, maximum output power, and end time.



Registration Process

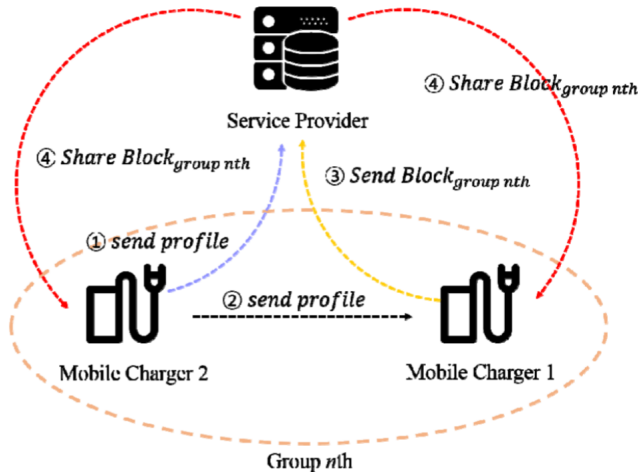


Transaction Communication

- The mobile charger transmits its Charging Profile to the service profile after charging.
- The mobile charger delivers all its charging profiles which occurred within the 'interval' value from idTagInfo to the parent node.
- The parent node that receives the profile of the group generates a block.
- If you get more than half the correct validation results for a transaction, the service provider adds the block to the existing Blockchain.
- The service provider checks the block information for billing and transmits the charge information according to the charge amount for each group



Sequence of transaction communication



Lightweight Blockchain data

- The proposed method is a re-construction of a block into a new type of block which is called Charge List Block.
- The service provider receives block for each group transaction from the parent node, and it re-constructs the block body part.
- If the size of the Blockchain data exceeds a certain size, it check the billing profile for the last transaction for each group.
- The block header of the Charge List Block is generated in the same way as the existing block header part, and is transmitted for each group.
- The group parent mobile chargers receive the newly created block form a new Blockchain starting from the reconstructed block.



Algorithm

Algorithm 1 : Block Data Size decrease

Input: *Whole Block*

Output: *Charge List Block*

1. Check Charging Data for each group
2. **for** number of group **do**
3. $CurrentBlockCharge$ per each group is '0'
4. **end for**
5. **do**
6. **for** number of group **do**
7. $i = 1$
8. $Charge_{G_i} = Charge_{G_i} + CurrentBlockCharge_{G_i}$
9. **End for**
10. $CurrentBlockCharge$ move to next Block
11. **while**(End of Block)
12. Generate Charge List Block
13. **for** number of group **do**
14. Add $Group_{id} + Charge_{G_i}$ to Block data
15. **end for**
16. Add $BlockHeader_{latest}$ and Block data
17. Send Charge List Block to each group parent node



Conclusion

- In order to provide efficient charging according to the charge details of the mobile charger, the mobile charger can be grouped by utilizing the groupId.
- In addition, using Blockchain technology, appropriate billing for charging can be generated.
- Moreover, I propose a technique to reduce the size of block data, and solve the problem of accumulating data size of existing Blockchain.

Reference

- Nam Ho Kim, Sun Moo Kang, Choong Seon Hong *“Mobile charger billing system using lightweight Blockchain”*, Sep. 2016.
- Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak *“BlockChain: A Distributed Solution to Automotive Security and Privacy”*, IEEE Communications Magazine, Vol. 55 , Issue. 6 , Dec. 2017
- Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven *“Bitcoin and cryptocurrency technologies: a comprehensive introduction”*, IEEE Communications Magazine, 2016



Reference

- Leonardo Aniello , Roberto Baldoni *“A Prototype Evaluation of a Tamper-Resistant High Performance Blockchain-Based Transaction Log for a Distributed Database”*, European Dependable Computing Conference (EDCC), Sep. 2017
- Michael Crosby et al, *Blockchain Technology: Beyond Bitcoin*, AIR (Applied Innovation Review), No. 2 ,June 2016
- Kenji Saito , Hiroyuki Yamada *“What’s So Different about Blockchain? — Blockchain is a Probabilistic State Machine”*, International Conference on Distributed Computing Systems Workshops, Jun. 2016
- Quoc Khanh Nguyen *“Blockchain - A Financial Technology for Future Sustainable Development”*, Conference on Green Technology and Sustainable Development (GTSD) Nov. 2016



Questions ?

Thank You