COM 5335 : NETWORK SECURITY

RESEARCH PAPER STUDY FINAL PROJECT

Delay and Communication Tradeoffs for BlockchainSystems With

Lightweight IoT Clients

Pietro Danzi , Student Member, IEEE, Anders E. Kalør , Student Member, IEEE,

Cˇ edomir Stefanovic´ , Senior Member, IEEE, and Petar Popovski , Fellow, IEEE

|  |  |
| --- | --- |
| **STUDENT ID :** | 108064535 |
| **NAME :** | Wen-Yuan Chen (Chris) |
| **PROFESSOR :** | Scott Huang |
| **SUPERVISOR :** | Thattapon Surasak |

1. INTRODUCTION

This following Table 1. will provide a brief explanation about this paper.

|  |  |  |
| --- | --- | --- |
| Q5 | Questions | Explanation |
| 1 | What is the research / telling question(s) ? |  |
| 2 | What are the key concepts ? |  |
| 3 | What methods are used ? |  |
| 4 | What answers are presented ? |  |
| 5 | What are the contributions of this paper ? |  |

Table 1. A brief explanation about this paper.

* What is blockchain ?

It’s a kind of database but it’s decentralized rather than centralized database. Which is mean the data is not held by a central server or central service whereas held by every node in the blockchain network. Hence, all blockchain nodes can stay on the top of data.

* Why we need blockchain technology ?

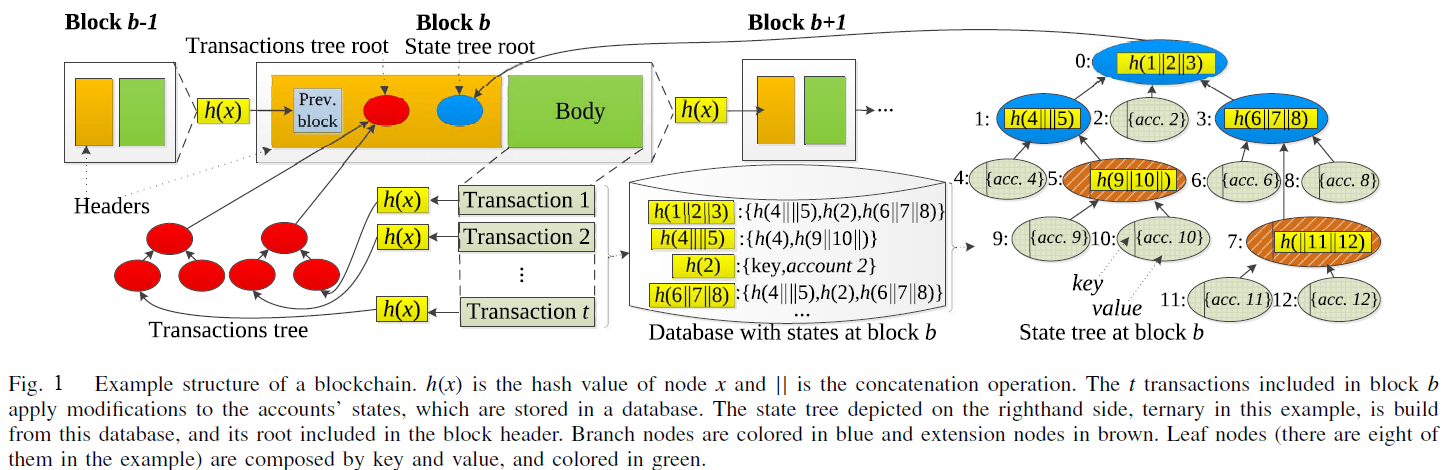
It’s aiming to support the implementation of decentralized applications (DAPPs). And these kind of applications will reduce the requirement of a central server to provide service and oversee the interactions between clients. Which is mean we don’t need to via a third party to complete a transaction whereas complete by ourselves. Furthermore, blockchain also has very strong security because all of transactions need to be validated by the nodes in the blockchain network according to the consensus algorithm.

* Blockchain protocol

The blockchain database is replicated at multiple nodes that are interconnected by a communication network. Every time a node appends a new block to its copy of the blockchain, it transmits the block to the rest of the other nodes in the network, to keep the blockchain database replications consistent.

* Block data structure for Ethereum

A block is consist of a block header and a body, you can reference Fig 1. The block header size is fixed, and the remainder parts of the block is composed of the actual transactions and have variable size. When the amount of transaction is high, the variable parts will almost account for the whole block.



* PoI via Merkle-Patricia Trees

Ethereum uses Merkle-Patricia Trees to provide Proof of Inclusion (PoI). Merkle-Patricia Trees have three types of nodes such as leaf, extension and branch nodes, you can reference right side of Fig 1.

* Synchronization protocols
* Problems from lightweight IoT devices

1. METHOD
2. RESULT
3. CONCLUSION
4. REFERENCE