Flowchain: A Distributed Ledger Designed for Peer-to-Peer IoT Networks and Real-time Data Transactions

Jollen Chen

January 20, 2017

Flowchain Open Source Project
jollen@jollen.org

Abstract. This paper proposes a distributed ledger system called Flowchain for peer-to-peer networks and real-time data transactions. Flowchain's significant feature is a Virtual Block that provides a new blockchain data structure design to improve the Satoshi blockchain structure and provide real-time transactions. Flowchain aims to address the blockchain system for the Internet of Things (IoT). Numerous blockchain systems, including the Satoshi blockchain, are intended to facilitate peer-to-peer currency transactions. Furthermore, "mining" is a mechanism and distributed consensus system that can verify and record such transactions. However, existing mining systems do not act specifically for the IoT. Thus, Flowchain employs Flowcoin to address such technical challenges. Flowcoin is a cryptocurrency system for trusted computing over peer-to-peer IoT networking. Flowchain provides a secure and real-time data exchange model for the IoT and ensures data privacy.

Keywords: Blockchain, Distributed Ledger, IoT, P2P, Cryptocurrency

1. Introduction

Blockchain for the Internet of Things (IoT) has considered a "black box." Despite a large number of studies on blockchain IoT, few studies have investigated how an IoT blockchain system works in practice. Flowchain represents an initial step toward an examination of the interoperability of IoT devices. IoT devices with peer-to-peer communication functions are interoperable. Furthermore, peer-to-peer communication is an important characteristic of the decentralized IoT model. The first technical challenge is how to design a peer-to-peer IoT network system. Blockchain for the IoT is the second challenge.

Completing a Bitcoin transaction may require approximately 15 minutes or longer because the mining process requires significant time. Given the current real-time data exchange ability of the IoT, it's nature that a different blockchain system is

used.The proposed Flowchain is a dedicated blockchain system for the IoT that can process and record transactions in a real-time manner. Flowchain presents a new mechanism called Virtual Blocks to provide such real-time transactions.

2. Flowchain Data Structure

As shown in Fig. 1, Bitcoin, a frequently referenced cryptocurrency, uses a distributed database system called a blockchain [1]. The blockchain is a distributed ledger system that records all verified and trusted transactions in blocks. The Bitcoin peer-to-peer network generates blocks and links the blocks as a chain.

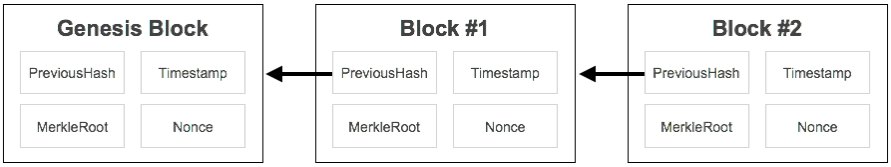

Fig. 1. Bitcoin blockchain structure

As shown in Fig. 2, Flowchain is a distributed ledger system for peer-to-peer IoT networks. Flowchain uses the Chord protocol and algorithm, a distributed hash table (DHT) technology published in 2001 by MIT [2]. WoT.City has presented a decentralized IoT software framework for a peer-to-peer and interoperable IoT device [3]. Consequently, Flowchain uses WoT.City as peer-to-peer IoT device middleware to construct the distributed ledger system.

Flowchain comprises a new blockchain data structure design and a cryptocurrency system for trusted computing to approach the secure data exchange required by the IoT. The proposed blockchain data structure is called Virtual Blocks, and it aims to provide real-time data transactions.

As shown in Fig. 3, the important Flowchain data structure design features are as follows.

- Five IoT devices are labeled N1 to N5, and each device is a “node” in a peer-to-peer network.
- All nodes are mining blocks that use the same genesis block.
- In other words, each node creates a new “branch” for mining; thus, there is no blockchain “fork.”
- Every block in each branch is called a Virtual Block.
- Virtual Blocks can be labeled as valid or invalid.
- Only valid blocks are available to record transactions.

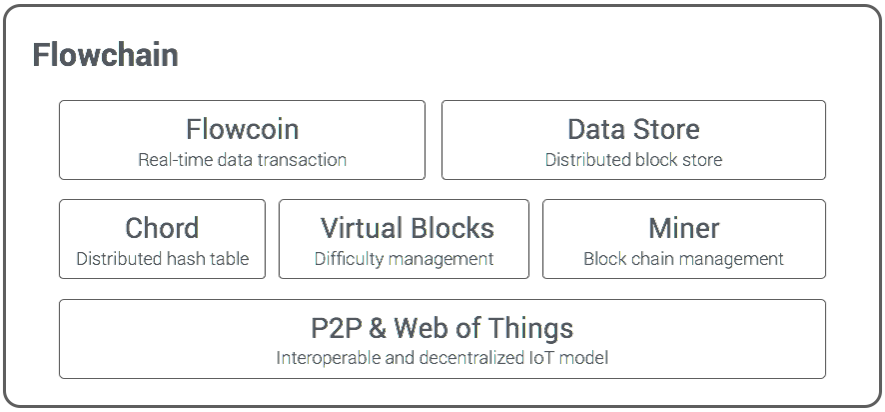

Fig. 2. The Flowchain system

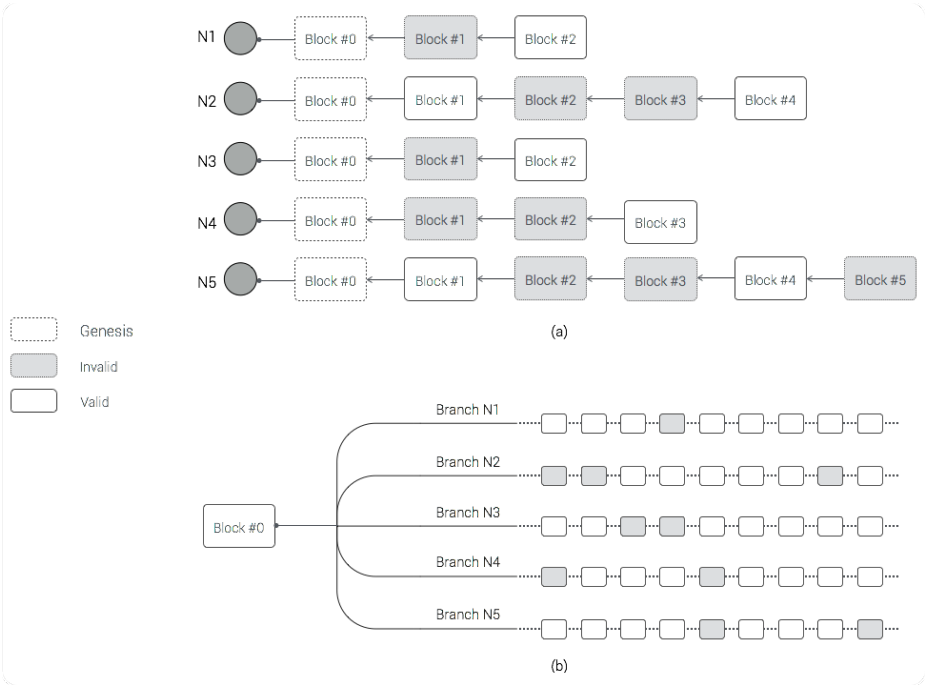

Fig. 3. Flowchain data structure

The most significant design feature of the Flowchain data structure is that every node can only mine blocks at its own branch. Therefore, Virtual Blocks do not need to be synchronized with all nodes because nodes do not "compete" to mine new blocks. Accordingly, Flowchain does not use a proof-of-work system [4].

Flowchain also proposes a mechanism called "Inventory" by which administrators can use dedicated branch merging algorithms to merge all branches into a single blockchain. For example, a Flowchain distributed ledger can be constructed by merging all branches with all their valid Virtual Blocks.

3. Mining and Difficulty

Flowcoin is a peer-to-peer distributed database that stores transactional data. In Flowcoin, the Virtual Block system can label blocks as valid or invalid. Valid blocks act as a secure ledger that stores transaction records.

Although Flowchain and Bitcoin use the same SHA-256 hash algorithm, Flowchain has a very different mining algorithm design. The proposed design allows an IoT device to operate more stably when mining blocks. In addition, IoT hardware varies, e.g., resource-constrained devices, mobile devices, and high-performance server frames; thus, their computing power is not equal. Consequently, the mining algorithm design should not be parallelized to avoid mining competition.

In addition, memory-hard hash functions [5], such as Argon2 [6], cannot be used in IoT devices. A resource-constrained device has limited computational power and memory; therefore, memory-hard hash functions do not perform well on IoT devices. As shown in Listing 1, a node receives a key-value pair through the peer-to-peer network and then stores it in a valid block.

Listing 1. Flowchain MRU block algorithm

```
Node.on('message', function(key, value) {
  // Get a valid block of the device's blockchain
  N = GetOneValidBlock(chains)

  // Put key-value pair in block "N"
  PutToBlock(N, {key: value});
});
```

Moreover, to reduce complexity relative to maintaining valid and invalid blocks, Flowchain proposes an O(1) implementation whereby only a single Most Recently Used (MRU) block is maintained. The MRU block is considered the only valid block in the "branch."

The implementation details of the MRU block algorithm differ from the application of the IoT, e.g, Flowchain can label the latest block as an MRU block. This

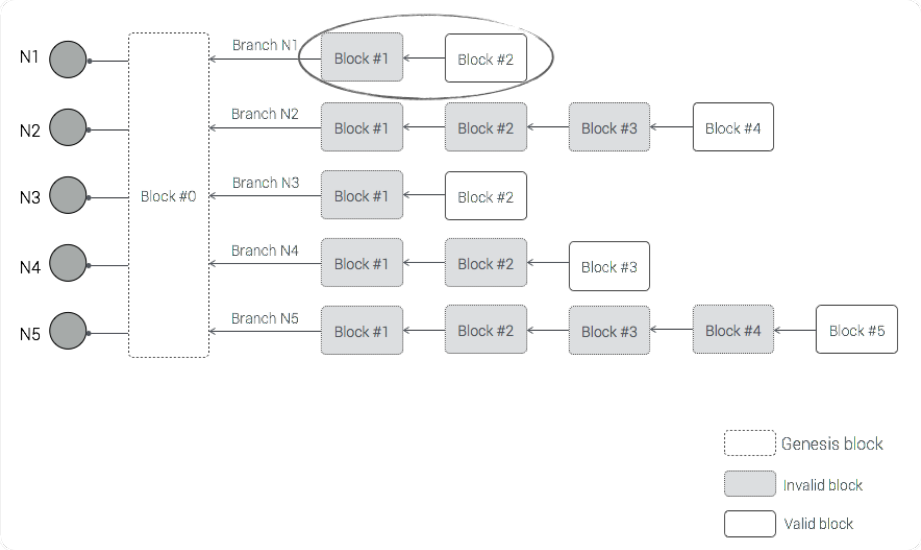

Fig. 4. Flowchain with a single valid block

means that all IoT devices will have only a single usable valid block. With this O(1) algorithm, the complexity issue could be resolved. In conclusion, Flowchain does not require hard-memory functions for devices with different computational power to avoid mining competition. As shown in Fig. 4, an optimized algorithm design that labels the latest block as the MRU block is shown.

Listing 2. Algorithm of Flowchain MRU block

```
Chord.on('message', function(key, value) {
  // N is the length of the blockchain.
  // Put payload in the latest block in the blockchain.
  // This is to say, only the latest block is valid for use.
  PutToBlock(chains[N-1], {key: value});
});
```

At the same time, the mining difficulty algorithm differs from the MRU block algorithm. Therefore, considering the algorithm shown in Listing 2, to collaborate with the algorithm design, Flowchain can use the probability density function of the normal distribution to determine the mining difficulty.

- A probability calculation can simply reference an IoT device's "reliability."
- Then, the reliability can be used as the variance input of the probability density function.

Borrowing the concept from the Bitcoin mining algorithm, a predefined difficulty table can easily implement such an algorithm. As shown in Listing 3, the leading zeros will increase the degree of difficulty. The mining becomes increasingly difficult with more leading zeros.

Listing 3. Mining difficulty table

```
Difficulties = [
  ‘0000FFFFFFFFFFFF’, // [0.0, 0.2)
  ‘000FFFFFFFFFFFFF’, // [0.2, 0.4)
  ‘00FFFFFFFFFFFFFF’, // [0.4, 0.6)
  ’0FFFFFFFFFFFFFFF’, // [0.6, 0.8)
  ’FFFFFFFFFFFFFFFF’  // [0.8, 1.0)
]
```

Thus, the miner can simply search the difficulty table and pick a value according to the probability. In addition, the miner is timed in a fixed number calculation per second in which the Flowchain can comprise a proof-of-stake mechanism.

4. Flowcoin: Peer-to-Peer Trusted Computing

Flowcoin, Flowchain’s cryptocurrency system, is responsible for real-time transactions and recording trusted data. Flowchain provides time-series and streaming data capabilities required by the IoT. Furthermore, each data slice in the time-series or streaming data is treated as a separate transaction, and Flowchain transfers each transaction to the peer-to-peer network. Thus, Flowcoin is a significant design element of Flowchain because it implements trusted peer-to-peer computing.

Each data slice is hashed by a double SHA-256 hash function to the corresponding data “key.” Chunk data comprise sliced data and the data key. Then, Flowchain forwards the chunk data to the chunk data’s “successor” node over the Chord ring. The Chord protocol and algorithm organize all IoT devices as a peer-to-peer network in a “ring” topology. The successor node lookup via the DHT with the data key processes the chunk data. This successor’s Flowcoin system creates a new transaction from the chunk data and stores it in a valid block after verification.

Moreover, given the data key’s hash generation algorithm, it is natural that the successor node is random and difficult to predict. In other words, the time-series and streaming data are distributed across IoT devices.

As shown in Fig. 5, the successor(key) is a function of the Chord algorithm that finds the data key’s node through the peer-to-peer network. The successor node is represented as N’.

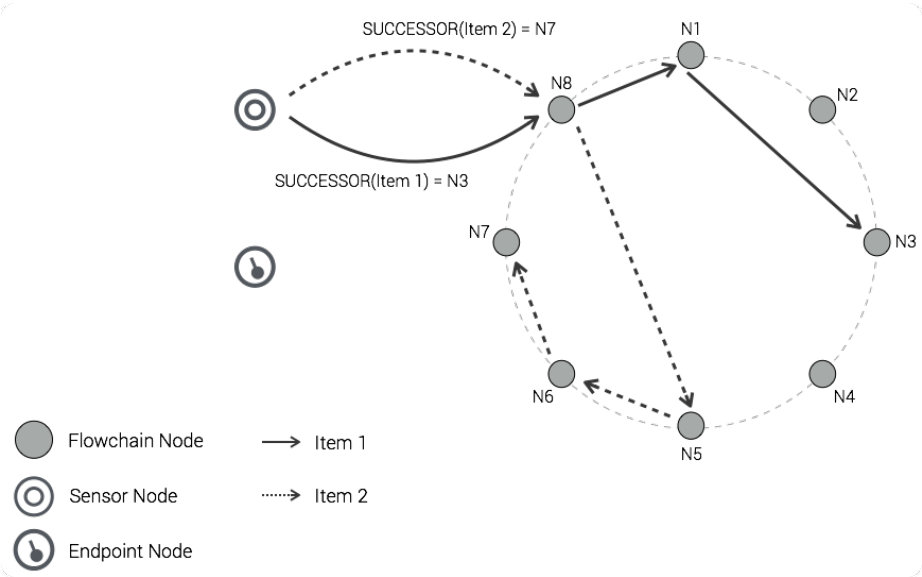

Fig. 5. Flowchain peer-to-peer networking

Listing 4. Flowcoin data transfer algorithm

```
N.put(data) {
  key = hashDataKey(data);

  // Send chunk data to N' through the Chord ring.
  send( SUCESSOR(key), { payload: data } );
}
```

Listing 5. Transaction generation algorithm

```
N'.PutToBlock(block, doc) {
  db = DatabaseAdapter.getDatabase();

  txId = SHA256( SHA256(block.id + doc.key) );

  txLabel = new Transaction(doc.value);
  txLabel.sign(privateKey);

  db.put({
    id: txId,
    label: txLabel
  });
}
```

When N' receives the chunk data, it combines the valid block ID and the data key to generate a transaction ID. To ensure data privacy, N' can also sign the transaction with its private key embedded in the hardware. Thus, N' stores the transaction ID and the chunk data in a valid block. The algorithm is shown in Listing 5.

As shown in Fig. 6, four simulated transactions from time-series data are forwarded to the peer-to-peer network in sequence. From the simulation process, it is obvious that the successor node of each transaction is unpredictable. Thus, this design helps to ensure data security.

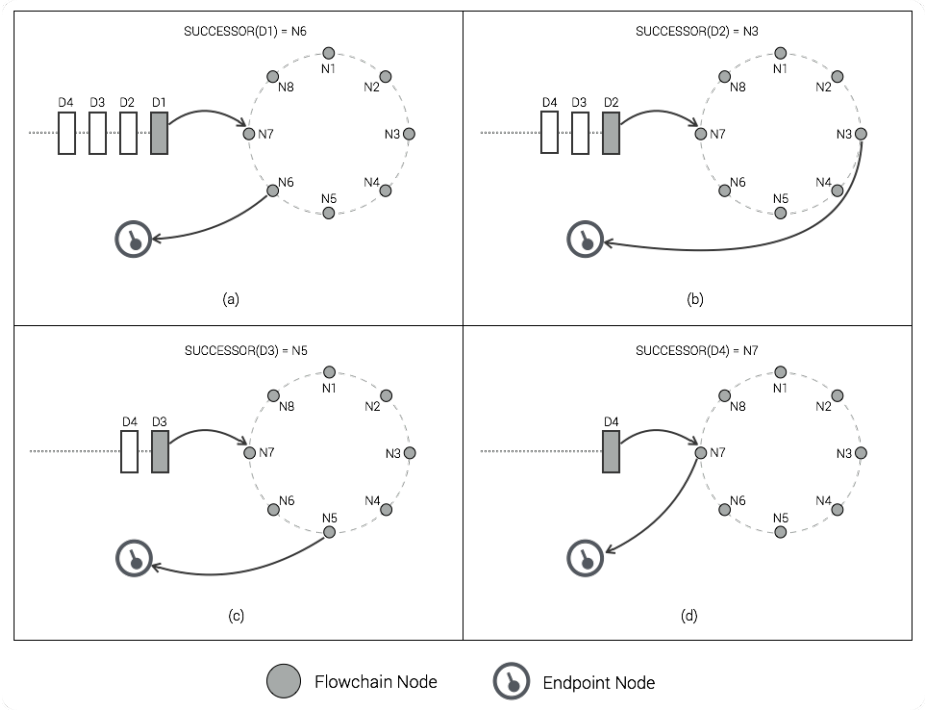

Fig. 6. Flowchain transactions

Differing from Bitcoin's transaction process [7], Flowchain uses a "mining-transaction-approval-verify" process rather than the typical "transaction-mining-verify" process. As shown in Fig. 7, in the process (6), N' forwards the chunk data to the endpoint after recording the transaction in the distributed ledger. At this time, this transaction has not been labeled as a "verified transaction." Subsequently, in process (7), the endpoint requests "approval" via one node of the peer-to-peer network. The previously mentioned transaction will only become a verified transaction if it is successfully verified by the peer-to-peer network. In

conclusion, Flowcoin will recognize the transaction as a verified transaction when the endpoint requests to approve it. Thus, the Flowchain transaction process represents a "mining-transaction-approval-verify" model. This mechanism is the most important Flowchain design element. Moreover, this mechanism attempts to provide a time-series and streaming data model for current IoT requirements.

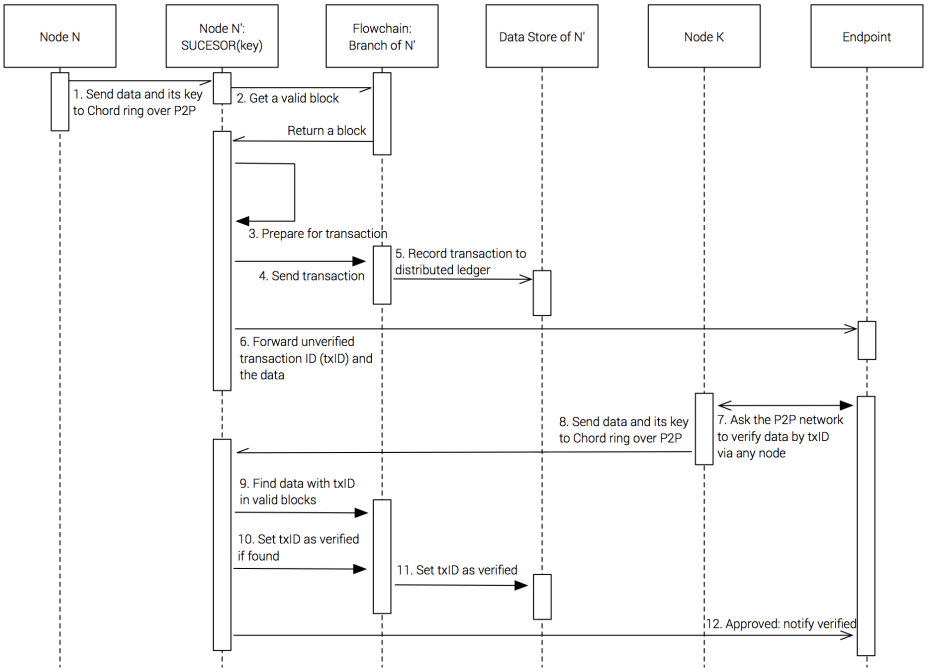

Fig. 7. Flowchain "mining-transaction-approval-verify" process

In addition, as shown in process (11) in Fig. 7, N' marks txID as verified after completing the approval request of the endpoint. Then, Flowchain grants one Flowcoin currency to N'. Note that N' can obtain more Flowcoin currency by completing more approval jobs.

In this manner, Flowcoin enables Flowchain to comprise a proof-of-stake [8] mining approach to mine new blocks. In other words, a node becomes more reliable when it is granted more "coins." The Flowchain difficulty algorithm uses the number of coins owned by a node to calculate the reliable probability.

In summary, chunk data are exchanged over the peer-to-peer network and are stored in the distributed data store between IoT devices. Flowchain ensures data security using its chunk data model and the data are distributed across all IoT devices. In addition, IoT device vendors can set up their own data privacy rules

for approval. Flowcoin is a cryptocurrency and trusted computing system with three major features:

- chunk data model to ensure data security;
- peer-to-peer IoT network cryptocurrency;
- "mining-transaction-approval-verify" model to provide real-time transactions.

In conclusion, Bitcoin uses a distributed single blockchain model in which all nodes compete to mine new blocks. In contrast, Flowchain initially creates branches for each node when nodes mine their own Virtual Blocks. This design also estimates block "forks" to maintain "valid and invalid blocks." Furthermore, Flowchain can create a branch merge operation in which all valid blocks of each branch can be merged into a single blockchain.

5. Conclusions

Flowchain employs an IoT dedicated blockchain design and implements the Flowcoin system for peer-to-peer IoT cryptocurrency and trusted computing. An IoT device can deposit "coins" by joining and completing "approval" jobs. To provide time-series and streaming data capabilities, Flowchain also employs the Virtual Block concept. Currently, the open source Flowchain project is available on GitHub [9]. Moreover, Flowchain has been ported to MediaTek LinkIt Smart 7688 IoT devices and has entered the practical proof-of-concept stage.

Future work. Flowchain will use a proof-of-stake system to determine device reliability. Device reliability determines mining difficulty. The peer-to-peer network validates resources for a node intending to join the network. The validation process ensures the node's minimum resource requirements, such as network bandwidth, battery level, and Wi-Fi signal strength.

6. References

1. Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto. https://bitcoin.org/bitcoin.pdf
2. Stoica, Morris (et al.): Chord: A scalable peer-to-peer lookup service for internet applications. ACM SIGCOMM Computer Communication Review. 31 (4): 149.
3. WoT.City white paper, https://wotcity.com/WoTCity-WhitePaper.pdf, 2017.
4. Proof-of-work system, https://en.wikipedia.org/wiki/Proof-of-work_system
5. Memory bound function, https://en.wikipedia.org/wiki/Memory_bound_function
6. The Argon2 document, https://github.com/P-H-C/phc-winner-argon2/blob/master/argon2-specs.pdf, 2016.

7. BlockChain Technology, http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf, 2015.
8. Sunny King and Scott Nadal. PPcoin: Peer-to-peer crypto-currency with proof-of-stake. https://wallet.peercoin.net/assets/paper/peercoin-paper.pdf, 2012.
9. Flowchain open source project, https://github.com/flowchain