A Hybrid Blockchain for the IoT and Tokenized Hardware

Jollen Chen, Founder & CEO, Flowchain

Beijing, China, June, 26, 2018
Jollen Chen is the creator and lead developer of Flowchain.io, an open source based IoT blockchain solutions. Before Flowchain.io, he has been working on embedded software and full-stack web development for many years. His research interests are the Distributed Ledger Technology (DLT) and IoT data security. Jollen holds a Master’s degree in Manufacturing Information and Systems from the National Cheng Kung University, Taiwan. You can find him online at http://jollen.org.
Flowchain
Quick Start
Flowchain Visions

Flowchain = (mining) * (IoT, Blockchain, AI)

- Cryptocurrency
  - (Incentives)
- Flowchain Technologies
The Distinguished Aspects

- Hardware/Software Development
- Blockchain designed from the ground up
- Proof-of-Concept via opensource
- Reviewed Research Papers
Free and Open

- Free and Open Source License
- Open Standards
- Web Technologies
- 100% JavaScript Implementations
Flowchain
A distributed ledger for the Internet-of-Things (aka. IoT Blockchain) in JavaScript

https://flowchain.co/  jolen@flowchain.io

Repositories 19  People 6  Teams 0  Projects 0  Settings

Pinned repositories

- **devify-server**
  A set of lightweight IoT cloud server boilerplates. The simplest way to build isomorphic JavaScript IoT servers.
  
  - JavaScript
  - 69 stars
  - 17 forks

- **flowchain-app**
  A Flowchain plugin that provides the flow-based programming (FBP) engine.

  - JavaScript
  - 26 stars
  - 5 forks

- **blockchain-starter-kit**
  The training course for better understanding the blockchain from the ground up: a project template to create as simple as possible implementation of a blockchain.

  - JavaScript
  - 42 stars
  - 18 forks

- **flowchain-ledger**
  A distributed ledger for the p2p and decentralized IoT devices in JavaScript.

  - JavaScript
  - 16 stars
  - 8 forks

- **wwRPC**
  A lightweight library that makes REST-style RPC operations over the Websocket

  - JavaScript
  - 3 stars
  - 2 forks

- **wotcity-wot-framework**
  Forked from wotcity/wotcity-wot-framework

  - JavaScript
The Flowchain Insides

- The dataflow blockchain
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI
The IoT nodes are self-organized as a “Ring”.

Exchange data (dataflows) over a p2p network.
Flowchain: A Distributed Ledger Designed for Peer-to-Peer IoT Networks and Real-time Data Transactions.


Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks

In Proceedings of the Workshop on 2nd Advances in IoT Architecture and Systems, June 3, 2018, Los Angeles, USA.
The Flowchain Insides

- The dataflow blockchain
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI
Blockchain OS, #2 of 4

- The flowchain OS called **Devify** enables Device Autonomous Machines

---

**Dextoken**: tokenized hardware and peer-to-peer trusted computing

**wwRPC**: the light-weight RPC over REST-style operations

**JavaScript Runtime**: (Node.js, V8, JerryScript, and etc.)
Flowchain OS runs **Everywhere**

- **Dapps**
- **RPC & DHT**
- **Thing (WoT)**
- **WebSocket / CoAP**

**Node.js 0.12**
- OpenWRT (Linux)
- MIPS Processor
  - 580MHz
  - 128MB DDR2
  - 32MB Flash

**JerryScript**
- FreeRTOS
- ARM Cortex-M4
  - 192MHz
  - 352KB RAM
  - 4MB Flash

**Node.js 4.4+**
- MacOS
- Intel Core 2
  - 1.4GHz
  - 2GB DDR3
  - 64GB SSD

**JavaScript**

**heterogeneous Hardware**
The Broker Server Layer

- A WoT Servient comprises of client and server combinations.
Content:

- **Where is PELE? Pervasive localization using wearable and handheld devices**
  Luis Henrik John¹, Chayan Sarkar², and R. Venkatesha Prasad¹
  ¹Delft University of Technology, Delft, The Netherlands
  ²TCS Research, Kolkata, India

- **Device Microagent for IoT Home Gateway: A Lightweight Plug-n-Play Architecture**
  Dhiman Chattopadhyay, Abinash Samantaray, and Anupam Datta
  Tata Consultancy Services, India

- **Automation of Feature Engineering for IoT Analytics**
  Snehasis Banerjee¹, Tanushyam Chattopadhyay¹, Arpan Pal¹, and Utpal Garain²
  ¹TCS Research & Innovation, Kolkata, West Bengal, India
  ²Indian Statistical Institute, Kolkata, India

- **Devify: Decentralized Internet of Things Software Framework for a Peer-to-Peer and Interoperable IoT Device**
  Jollen Chen
  Devify, Inc., Devify Open Source Project

- **Zero Energy Visible Light Communication Receiver for Embedded Applications**
  Prabhakar T V¹, Vishwas Shashidhar², G S Aishwarya Meghana², R. Venkatesha Prasad³, and Garani Vittal Pranavendra⁴
  ¹Indian Institute of Science, Bangalore, India
  ²NITK, Surathkal, Mangalore, India
  ³Delft University of Technology, Delft, The Netherlands
  ⁴Indian Institute of Technology, Bhubaneswar, India

Editorial Board:
- Sergiy Bogomolov, Australian National University, Australia
- Oleg Sokolsky, University of Pennsylvania
The Flowchain Insides

- The dataflow blockchain
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI
Hybrid Blockchain, #3 of 4

- The Flowchain comprises of a public blockchain and multiple private blockchains.
- The hybrid consensus nodes implement such hybrid blockchain model.

![Hybrid Blockchain Diagram]

1. **AI Edge Computing**
   - N1
   - N2
   - N3
   - N4
   - N5
   - N6
   - N7
   - N8

2. **Distributed AI Computing Pool**
   - Flowchain Pool
   - Hybrid Consensus
• Flowchain IoT nodes are devices that running Flowchain code.

• Puzzles Miner is a computer that aims to generate the *puzzles* and broadcasts the puzzles to the private blockchains.
The Flowchain Insides

- The dataflow blockchain
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI
Decentralized AI, #4 of 4

AI Miners & AI Computing Pool
Flowchain
Pseudonymous Authentication
IoT Blockchain + AI over Pseudonymous Authentication

Private Blockchain B
Flowchain IoT Nodes

Private Blockchain A
Flowchain IoT Nodes

Private Blockchain C
Flowchain IoT Nodes

Private Blockchain D
Flowchain IoT Nodes

Trusted Transactions

Puzzle Miners
Public Blockchain

Trusted Transactions
Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks

ABSTRACT

The Internet of Things (IoT) device has a number of challenges, ranging from the need to exchange data securely, authenticate devices, and manage data privacy. However, the current blockchain technology is not well-suited for self-encrypting devices, which are constrained in terms of computing power, memory, and storage. This paper addresses these challenges by proposing a hybrid blockchain design that enables secure and trusted IoT communications. The proposed blockchain technology is designed to address the limitations of traditional blockchain technologies, such as those used in cryptocurrencies, by allowing devices to exchange data securely while minimizing the computational and storage requirements.

Keywords: Internet of Things, Blockchain, Pseudonymous Authentication, Hybrid Blockchain

1. INTRODUCTION

The Internet of Things (IoT) is a network of physical devices connected to the internet that can uniquely identify themselves and exchange data. The IoT has the potential to transform industries and improve the quality of life by enabling smarter and more efficient systems. However, the IoT is also facing several challenges, including security and privacy issues. Blockchain technology is a promising solution to address these challenges, as it provides a secure and transparent way to exchange data. However, traditional blockchain technologies are not well-suited for IoT devices due to their high computational and storage requirements.

1.1 Previous Works

In recent years, several blockchain-based solutions have been proposed to address the challenges of the IoT. These solutions include Flowchain [7] and Devify [12]. Flowchain is a blockchain technology for the IoT that is designed to enable secure and trusted device communications. Devify is a decentralized software framework for building various types of trust IoT networks by using a p2p network and the concept of the blockchain. In our previous work, Flowchain has also already proposed an IoT blockchain for the IoT, which is designed to enable trustless communications for the IoT and provide the capabilities for our hybrid blockchain design.

1.2 Type of Blockchains

Blockchain technology can be classified into two main types: public and private. Public blockchains, such as Bitcoin and Ethereum, use proof-of-work (PoW) consensus mechanisms to ensure the security and integrity of the blockchain network. Private blockchains, on the other hand, use proof-of-stake (PoS) mechanisms to ensure the real-time transactions for IoT devices. However, traditional blockchain technologies are not well-suited for IoT devices due to their high computational and storage requirements.

1.3 Blockchain

Blockchain technology is a distributed database that records transactions in a secure and transparent way. Each transaction is recorded in a block, which is added to the blockchain. The blockchain is maintained by a network of nodes, which are responsible for verifying and adding new blocks to the chain. However, traditional blockchain technologies are not well-suited for IoT devices due to their high computational and storage requirements.

1.4 Type of Blockchains

Blockchain technology comprises of a p2p network system, and a consensus algorithm that can enable trustless communications for the IoT and provide the capabilities for our hybrid blockchain design. The traditional public blockchain technology is not well-suited for IoT devices due to their high computational and storage requirements. However, blockchain technology has the potential to address the challenges of the IoT and enable secure and trustless communications. However, traditional public blockchain technologies are not well-suited for IoT devices due to their high computational and storage requirements.

2. PROPOSED BLOCKCHAIN DESIGN

The proposed blockchain design is based on a hybrid model that combines the benefits of both public and private blockchain technologies. The hybrid blockchain design is designed to enable trustless communications for the IoT and provide the capabilities of a public blockchain, while minimizing the computational and storage requirements of private blockchain technologies. The hybrid blockchain design is based on a combination of traditional blockchain technologies and pseudonymous authentication mechanisms. The proposed blockchain design is designed to enable secure and trustless communications for the IoT by using a p2p network system and a consensus algorithm.
Anyone can join the blockchain network that the blockchain network is completely open to users for submitting transactions.

The public blockchain can enable a decentralized model that it can operate without any central authorizations; thus the public blockchain has the natures of openness and trust.
Private Blockchains

Only authenticated users can join the private blockchain network.

The user need to request permissions from an authority in the private blockchain for joining the network and submitting transactions to the private blockchain network.
Pseudonymous authentication can replace the PKI to enable a fast authentication.
**Puzzle Miner** is a scheduler that provides time-difficulty string search puzzles

The IoT node was pseudonymously authenticated to submit transactions at \((t_i, t_j, t_k)\).

**Fix period scheduling:** 1 second = 50.0 slices (50 kHz)
a truly random Konami Code that only validate in a fixed time period
Lambda.prototype._miner = function() {
    var MAX_LOOPS = 1000000;  // 1M

    // FIXME: the difficulty has to be a small number of a shared difficulty from the public mining pool
    var difficulties = [
        '00F8888888888888888888888888888888888888888888888888888888888888',
        '0F88888888888888888888888888888888888888888888888888888888888888'
    ];

    var nonce = this.nonce;

    while (MAX_LOOPS--> 0) {
        var hash = virtualMiner(nonce, this.sHeaderHash, this.sSeedHash);

        if (hash <= difficulties[0]) {
            console.log(chalk.green('New block found: 0x' + hash.toString(16)));
            this.nonce = nonce;
            return nonce;
        }
        nonce++;
    }

    console.log('Cannot found a valid lambda value. Please try again later.');
    return 0;
}

function Lambda() {
    this.sHeaderHash = ";
    this.sSeedHash = ";
    this.sShareTarget = ";
    this.nonce = 1;
    return this;
}
var virtualMiner = function(nonce, previousHash, seedHash) {
    // The header of the new block.
    var header = {
        nonce: nonce,
        seed: seedHash,
        previousHash: previousHash,
        timestamp: new Date()
    };

    var blockHash = crypto.createHmac('sha256', 'Flowchain is magic ;-)')
        .update( JSON.stringify(header) )
        .digest('hex');

    // Generate the lambda value and its corresponding puzzle.
    gLambda.generateLambdaPuzzle(nonce, header);

    return blockHash;
};
Puzzle Miner algorithm

1. $Ui$ starts receiving $\lambda$ from the broadcasting
2. Let $\text{Puzzle}$ be a function and $\xi_j$ be a string; $Ui$ receives a puzzle ($\text{Puzzle}, x_j$) from a peer $Uj$ in the private blockchain over the p2p network
3. Let $\text{Puzzle}(\lambda)$ gives an arbitrary-length vector $\vec{x}$ of the Konami Code, then $\vec{x} = (x_1, \ldots, x_n), n < j$
4. Let $\mathcal{F}_{puz}$ maintain a set $\mathcal{T}$ of puzzle solutions, then $\mathcal{F}_{puz}$ computes each entries in $\vec{x}$, let $y_i = \mathcal{F}_{puz}(x_i), i = (1, \ldots, j)$
5. The miners say that $Ui$ solves the puzzle ($\text{Puzzle}, x_j$) if $\mathcal{F}_{puz}$ successfully finds $y_i = x_j$ within the time interval $\sigma$
6. $\mathcal{F}_{puz}$ returns $\xi_j$ to $Uj$ and stores $\mathcal{H} = (\vec{x}, y_i, \lambda)$ in $\mathcal{T}$
7. The miners and $Uj$ confirm the user $Ui$ is authenticated
Lambda.prototype `generateLambdaPuzzle` = function(nonce, header) {
    var SeqList = require('seqlist');
    var crypto = require('crypto');

    // FILL YOUR TOKEN ADDRESS
    var hash = crypto.createHmac('sha256', '0xA3b2692eD05309a33F589cDb197767bc257D7C2B')
        .update(JSON.stringify(header))
        .digest('hex');
    var arr = hash.split('');
    var seqlist = new SeqList(arr);

    var q1 = seqlist.topk(10, 'max');
    var q2 = seqlist.topk(10, 'min');

    var lambda = hash.replace(q1, '');//
    var puzzle = {
        q1: q1,
        q2: q2
    };

    this.lambda = lambda;
    this.puzzle = JSON.stringify(puzzle);

    console.log('Hash #' + hash);
    console.log('  Generated puzzle #' + this.puzzle);
    console.log('  Generated lambda #' + this.lambda);
};
Submit transactions to the public blockchain for verification.

1. The trusted user $U_i$ produces a message or receives a message from another user through the p2p network; formally, let $M$ be this message.
2. The trusted user $U_i$ has the keypair $(sk_i, pi_i)$; let $Sign$ be the signature function.
3. Let $T_i$ be the new transaction and $Hash$ be a hash function so that $T_i = Hash(Sign(M), H, pk_i)$;
4. $U_i$ submits $T_i$ to the public blockchain.
Byzantine Fault Tolerance

- \( n = 8 \)
- \( \pi = 1 \)
- \( n > 3\pi + 1 \)
- for \( n \) in \([N1..N8)\)
  \[ f_{\text{conn}}(n) > 2\pi + 1 \]
Flowchain BFT

$n = 8$

$\pi = 1$

$n >= \pi + 1$

Faulty PEs free
Finding top-$k$ elements in data streams

Nuno Homem *, Joao Paulo Carvalho

TULisbon – Instituto Superior Técnico, INESC-ID, R. Alves Redol 9, 1000-029 Lisboa, Portugal

Fig. 10. Top-$k$ Precision with increasing space in Trials 5.
基於 BFT 的共識算法

<table>
<thead>
<tr>
<th></th>
<th>Dolev</th>
<th>Fekete</th>
<th>FCA</th>
<th>CCA</th>
<th>Flowchain BFT</th>
<th>Brooks-Iyengar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum faulty PEs</td>
<td>N/3</td>
<td>N/4</td>
<td>N/3</td>
<td>N/3</td>
<td>N/2</td>
<td>N/3</td>
</tr>
<tr>
<td>Complexity</td>
<td>Nπ</td>
<td>N/A</td>
<td>O(</td>
<td>N/A</td>
<td>O(</td>
<td>O(</td>
</tr>
<tr>
<td>Order of network bandwidth</td>
<td>O(N)</td>
<td>O(</td>
<td>O(N)</td>
<td>O(</td>
<td>O(N)</td>
<td>O(N)</td>
</tr>
<tr>
<td>Convergence rate</td>
<td>1/(N-2π-1)</td>
<td>1/((N-2π)/π)</td>
<td>2π/N</td>
<td>π/N</td>
<td>2*accuracy</td>
<td>2π/N</td>
</tr>
</tbody>
</table>
Trust and Anonymity

Permissioned
- PoS, DPoS
- Kafka

Permissionless
- PoW
- PoET

Public
- FlowchainBFT

Private
- PBFT, SBFT
- Multi-signature

FBA, Quantum

Source: https://flowchain.co
Flowchain
Submit
Transactions
Flowchain Node

Endpoint Node

SUCCESSOR(D1) = N6

SUCCESSOR(D2) = N3

SUCCESSOR(D3) = N5

SUCCESSOR(D4) = N7

(a)  

(b)  

(c)  

(d)  

Flowchain Node  Endpoint Node
Flowchain P2P Dataflows

- Wireless Sensor Network (WSN) over the decentralized and peer-to-peer network.
- N8 is the “broker service” of Sensor-8.
- N7 is the “successor node” of “Data 1” gathered by Sensor-8.
Generating Data Key

- Use SHA1
- The $H_{\text{DATA}}$ is the hash key of “sensor data”

$$H_{\text{DATA}} = \text{SHA1}( \text{data} + \text{timestamp} + \text{random} )$$

**SUCESSOR($H_{\text{DATA}}$):**
Lookup the successor node in the DHT
Generating Transaction ID

- Use SHA256, SHA1, and Double SHA256
- The $H_{DATA}$ hash is generated by the p2p network

\[
H_{BLOCK} = \text{SHA256}( \text{BlockNo} + \text{timestamp} + \text{nonce} )
\]
\[
H_{DATA} = \text{SHA1}( \text{data} + \text{timestamp} + \lambda )
\]
\[
H_{txID} = \text{SHA256}( \text{SHA256}( H_{BLOCK} + H_{DATA} ) )
\]
Data Transactions

• **The data transaction process (E)**
  
  • Step 1: Generate the key of the data - $H_{DATA}$
  
  • Step 2: Search the successor node of the key in the DHT - $\text{SUCCESSOR}(H_{DATA})$
  
  • Step 3: Send $[H_{DATA}, \lambda]$ to the successor node over the RPC operations
  
  • Step 4: The successor node generates $H_{txID}$
  
  • Step 5: The successor node signs (optional) and submits $H_{txID}$ to the public blockchain
Authenticated Encryption with Associated Data (AEAD)

The puzzle solution

A

E

encrypted

authenticated
Flowchain
Tokenized Hardware
Cooperate on Tokenized Hardware

The first paper to propose **Tokenized Hardware** and deep intuitive understanding of the next wave of hardware industry.

Flowchain and Seeed Studio press Tokenized Hardware position paper, expected to enter an entirely new level of IoT and Blockchain engagement products.
Eric Pan, the famous and 30 under 30 entrepreneur in Chain, has deep experience and knowledge in hardware industry. He is the Founder and CEO, Seeed Studio, a leading open source hardware supplier in the world.

Jollen Chen, the open source developer, has deep experience and knowledge in embedded software industry. He is the Founder of Flowchain, a IoT blockchain software company in Taiwan.
FlowchainCoin (FLC) is an utility token that can be used in tokenizing hardware and accessing the Flowchain platform.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>v.s.</th>
<th>Tokenized Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tangible assets</td>
<td></td>
<td>• Tangible assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Digital assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ownership</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Depreciation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Externality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Decentralized assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exchange (Dextoken)</td>
</tr>
</tbody>
</table>

From Hardware to Tokenized Hardware
Conclusions
Trusted thirty parties removed by Flowchain using the blockchain technologies

The data flow can be safely sent through an untrusted channel is trustless communication.
The Flowchain Model

- Trusted Hardware
- Trustless Communication and Consensus
- Distributed Autonomous Machines
- The AI Dapps
**Flowchain** underlying layer: Tokenized Hardware + DAM

<table>
<thead>
<tr>
<th>Secure input and output</th>
<th>Current Trusted Computing Model</th>
<th>Flowchain Trustless Computing Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARM TrustZone Virtualization Linux</td>
<td>Tokenized &amp; Trusted Hardware</td>
<td></td>
</tr>
<tr>
<td>Memory curtaining / protected execution</td>
<td>Cryptography</td>
<td></td>
</tr>
<tr>
<td>Endorsement key</td>
<td>DRM</td>
<td></td>
</tr>
<tr>
<td>Sealed storage</td>
<td>Distributed Autonomous Machines</td>
<td></td>
</tr>
<tr>
<td>Remote attestation</td>
<td>CA PKI HMAC</td>
<td></td>
</tr>
<tr>
<td>Trusted Third Party (TTP)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Flowchain** uppermost layer: AI over IoT Blockchain

Tokenized Hardware & Distributed Autonomous Machines

Data Models & Datasets

Machine Learning Miners & Incentives

Trusted Transactions

Private Blockchain

Flowchain IoT Nodes

Public Blockchain

Miners
Flowchain = (mining) * (IoT, Blockchain, AI)

Website: https://flowchain.co
Github: https://github.com/flowchain
Contact: jollen@flowchain.io
WeChat: jollentw