A Hybrid Blockchain for the IoT and Tokenized Hardware

Jollen Chen,
Founder and CEO
The Flowchain Foundation

The Linux Foundation,
Open Source Summit Japan,
Tokyo, June, 20, 2018
About me

Jollen Chen,
Founder & CEO,
The Flowchain Foundation

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.
The History and Roadmap

2015
- Ideas

2016
- Web of Things (WoT) Framework

2017
- IoT Blockchain upon the WoT framework

2018
- Tokenized Hardware and AI over IoT Blockchain
- ICO: Private Sale and Pre-allocation

2019
- ICO: Crowd Sale
- Global Market

FLOWCHAIN
Flowchain
Quick Start
Flowchain Visions

Flowchain = ((3rd platforms) \times (IoT, Blockchain, AI))

Partnership

1 + 1 > 2

Flowchain Technologies
The Distinguished Aspects

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

FLOWCHAIN
Free and Open

- Open Source License
- Open Standards
- Web Technologies
- 100% JavaScript Implementations
Academic Papers

Devify: Decentralized Internet of Things Software Framework for a Peer-to-Peer and Interoperable IoT Device.


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.
Github Repositories

Flowchain
A distributed ledger for the Internet-of-Things (aka. IoT Blockchain) in JavaScript
https://flowchain.co/  jollen@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  ★ 17

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

  - JavaScript  ★ 26  ★ 5

- 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  ★ 18

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

  - JavaScript  ★ 16  ★ 8

- wwRPC
A light weight library that makes REST-style RPC operations over the Websocket

  - JavaScript  ★ 3  ★ 2

- wotcity-wot-framework
Forked from wotcity/wotcity-wot-framework
wotcity.io: the Web of Things programming framework

  - JavaScript
The Flowchain Insides

- The dataflow blockchain
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI
**Dataflow** Blockchain, #1 of 4

- The IoT nodes are self-organized as a “Ring”.
- Exchange data (dataflows) over a p2p network.
The flowchain OS enables Device Autonomous Machines

**Blockchain OS, #2 of 4**

- **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.)**
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.
Decentralized AI, #4 of 4

AI Computing Center & AI Computing Pool

Company A (Flowchain Edge AI)
Company B (Flowchain Edge AI)
Company C (Flowchain Edge AI)
Company D (Flowchain Edge AI)
Company E (Flowchain Edge AI)
Company F (Flowchain Edge AI)
Flowchain
Hybrid Blockchain
Public Blockchains

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.
• 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.
Flowchain Operating System (OS)

- Trusted Assets Storage
- Digital Assets Management
- Tokenized Things Management
- Decentralized Exchange (DEX)

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

- Virtual Block
- Miner
- P2P Protocol
- Distributed Hash Table

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

- Event Emitter
- URL Router
- Request Handlers
- Thing Description

**Application LayerProtocols**

- JavaScript Runtime (Node.js, V8, JerryScript, and etc.)
Architecture Design

- **Distributed Ledger Layer**
  - Usually known as the “Blockchain”
  - Provides a distributed data store that shares transactional data across all IoT devices

- **Broker Server Layer**
  - Provides a helper library to create the IoT application server and establishes the peer-to-peer IoT networking

- **Web of Things (WoT) Layer**
  - Adopts the W3C’s WoT ontology that represents the physical IoT device as a virtual object
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.
Flowchain

Algorithms
P2P Geography over Chord

Figure: A 16-node Chord network. The "fingers" for one of the nodes are highlighted. License: CC BY-SA 3.0. Source: https://en.wikipedia.org/wiki/Chord_(peer-to-peer)
SUCCESSOR(D1) = N6

SUCCESSOR(D2) = N3

SUCCESSOR(D3) = N5

SUCCESSOR(D4) = N7

Flowchain Node
Endpoint Node

FLOWCHAIN

(a) (b) (c) (d)
Flowchain Decentralized WSN

- 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 $H_{DATA}$ is the hash key of “sensor data”

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

**SUCESSOR( $H_{DATA}$):**
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

$H_{BLOCK} = SHA256( \text{BlockNo} + \text{timestamp} + \text{nonce} )$

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

$H_{txID} = SHA256( SHA256( H_{BLOCK} + H_{DATA} ) )$
Data Transactions

- The data transaction process
  - Step 1: Generate the key of the data - $H_{DATA}$
  - Step 2: Search the successor node of the key in the DHT - SUCCESSOR($H_{DATA}$)
  - Step 3: Send $[H_{DATA}, \text{Konami Code}]$ 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
Hybrid Flowchain: IoT Blockchain + AI over Pseudonymous Authentication

Private Blockchain B
Flowchain IoT Nodes

Private Blockchain A
Flowchain IoT Nodes

Private Blockchain C

Private Blockchain D

Flowchain IoT Nodes

Trusted Transactions

Puzzle Miners

Public Blockchain

Trusted Transactions
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)
Puzzle Miner algorithm

1. $U_i$ starts receiving $\lambda$ from the broadcasting
2. Let $\text{Puzzle}$ be a function and $x_j$ be a string; $U_i$ receives a puzzle $(\text{Puzzle}, x_j)$ from a peer $U_j$ 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 $U_i$ 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 $x_j$ to $U_j$ and stores $H = (\vec{x}, y_i, \lambda)$ in $\mathcal{T}$
7. The miners and $U_j$ confirm the user $U_i$ is authenticated
a truly random Konami Code that only validate in a fixed time period
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
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.
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>v.s.</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>
Conclusions
How can apps trust the data sent from an arbitrary device?

Decentralized is impossible if we have to use trusted third parties.
Trusted third 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

The AI Dapps

Distributed Autonomous Machines

Trustless Communication and Consensus

Trusted Hardware
# Flowchain underlying layer: Tokenized Hardware + DAM

<table>
<thead>
<tr>
<th>Feature</th>
<th>Current Trusted Computing Model</th>
<th>Flowchain Trustless Computing Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure input and output</td>
<td>ARM TrustZone Virtualization Linux</td>
<td>Tokenized &amp; Trusted Hardware</td>
</tr>
<tr>
<td>Memory curtaining / protected execution</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>Endorsement key</td>
<td>Cryptography</td>
<td></td>
</tr>
<tr>
<td>Sealed storage</td>
<td>DRM</td>
<td>Distributed Autonomous Machines</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