FLOWCHAIN

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

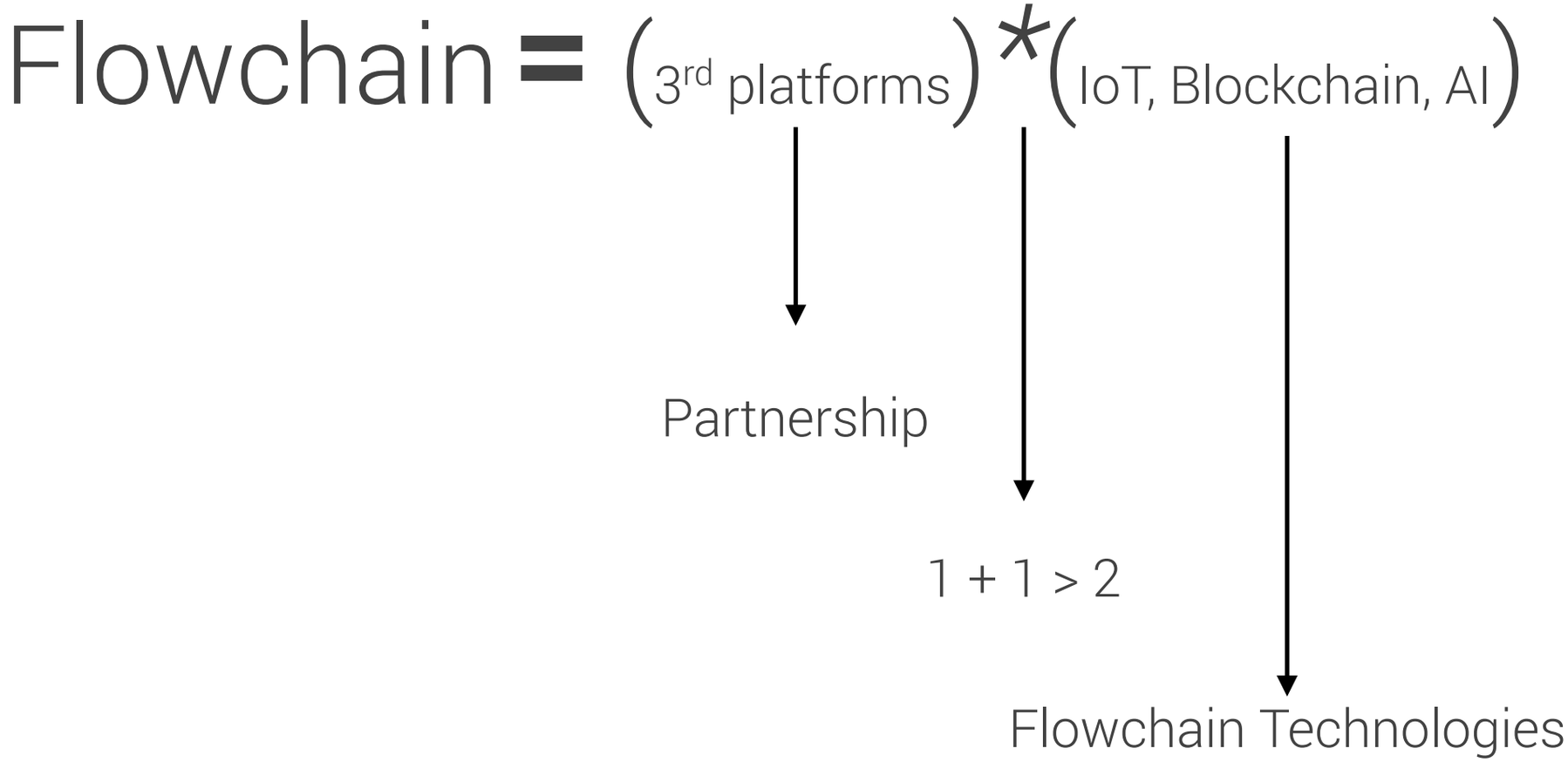
2019 ICO: Crowd Sale
Global Market

FLOWCHAIN

Flowchain

Quick Start

Flowchain Visions

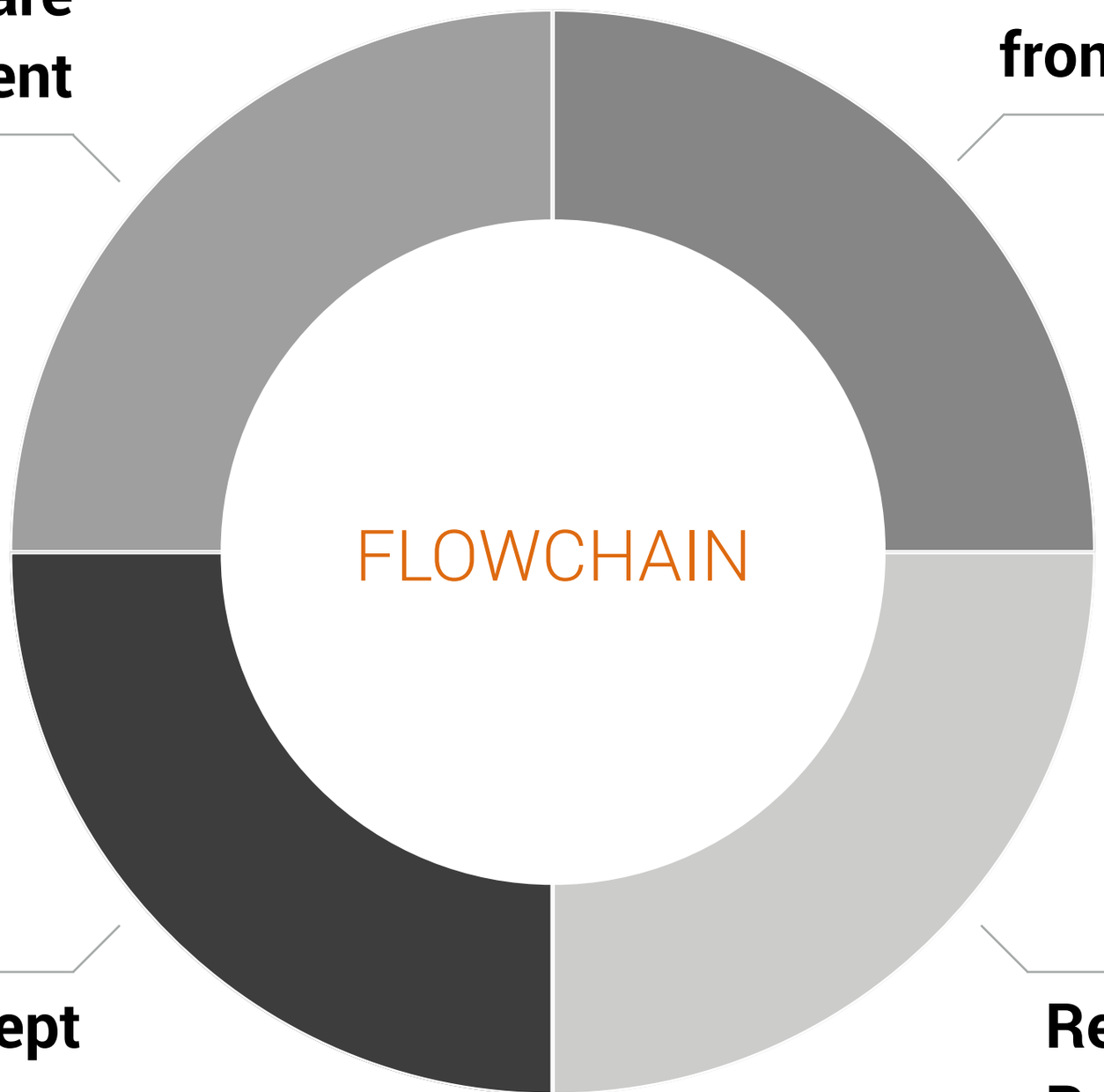


FLOWCHAIN

The Distinguished Aspects

Hardware/Software Development

Blockchain designed from the ground up



Proof-of-Concept via opensource

Reviewed Research Papers

Free and Open

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

FLOWCHAIN

Academic Papers

Reviewed Research Paper

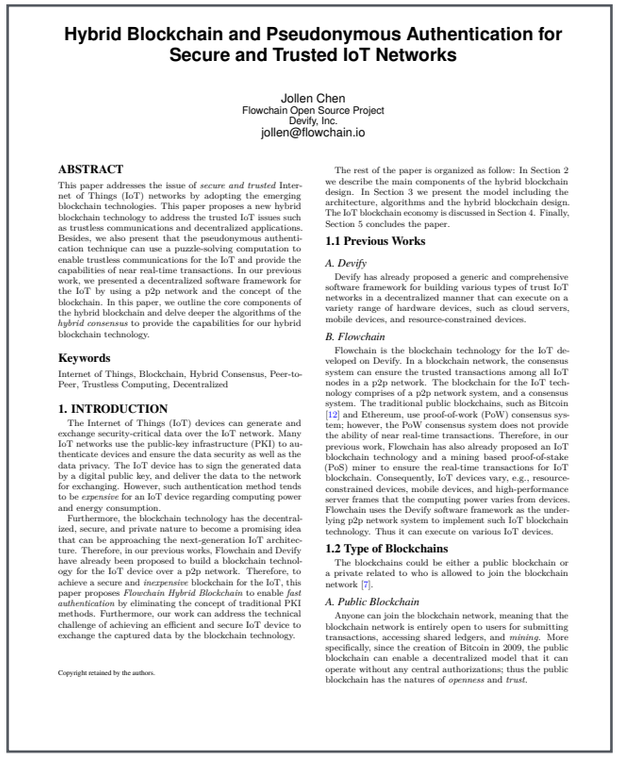
Devify: Decentralized Internet of Things Software Framework for a Peer-to-Peer and Interoperable IoT Device.

Reviewed and published in the Workshop on Advances in IoT Architecture and Systems, June 25, 2017, Toronto, Canada.

Reviewed Research Paper

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

Reviewed and published in the 2nd International Workshop on Linked Data and Distributed Ledgers, May 29, 2017, Portoroz, Slovenia.



Reviewed Research Paper

Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks

InProceedings 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

Customize 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

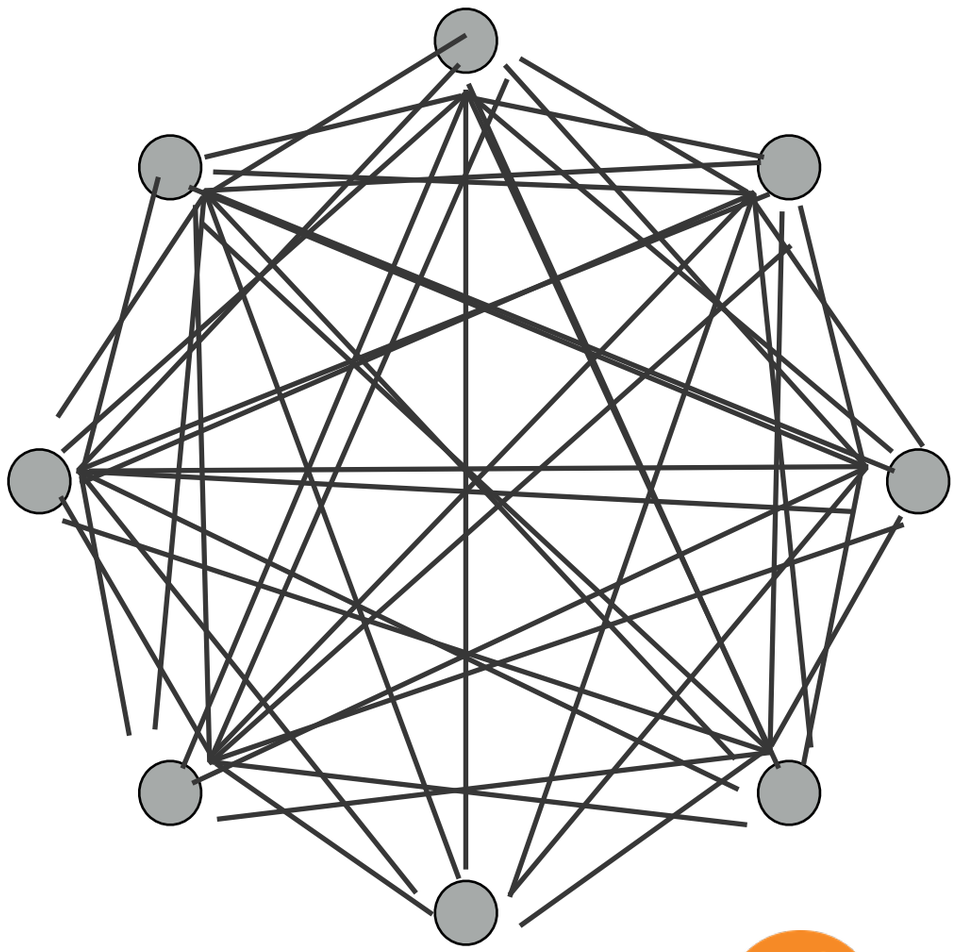
The Flowchain Insides

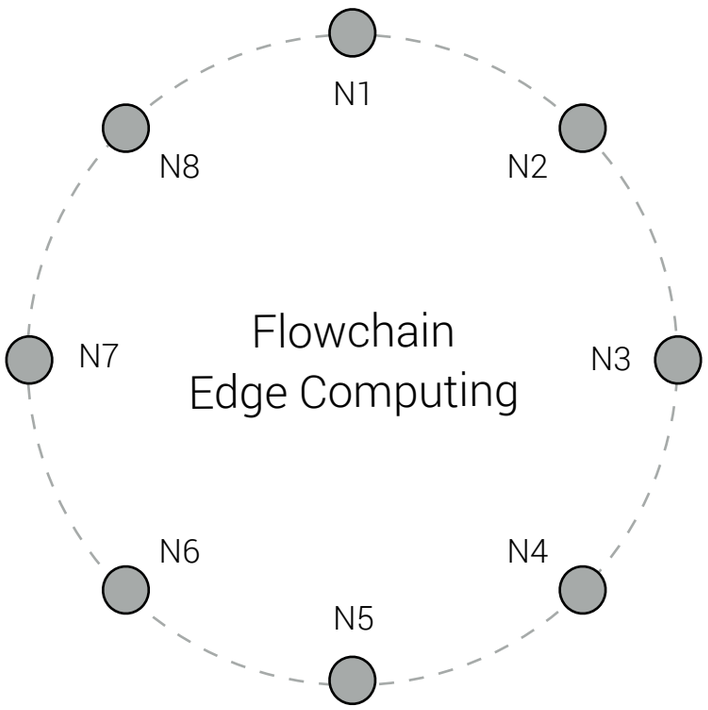
- The data**flow** block**chain**
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI

FLOWCHAIN

Dataflow Blockchain, #1 of 4

- The IoT nodes are self-organized as a “Ring”.
- Exchange data (dataflows) over a p2p network.



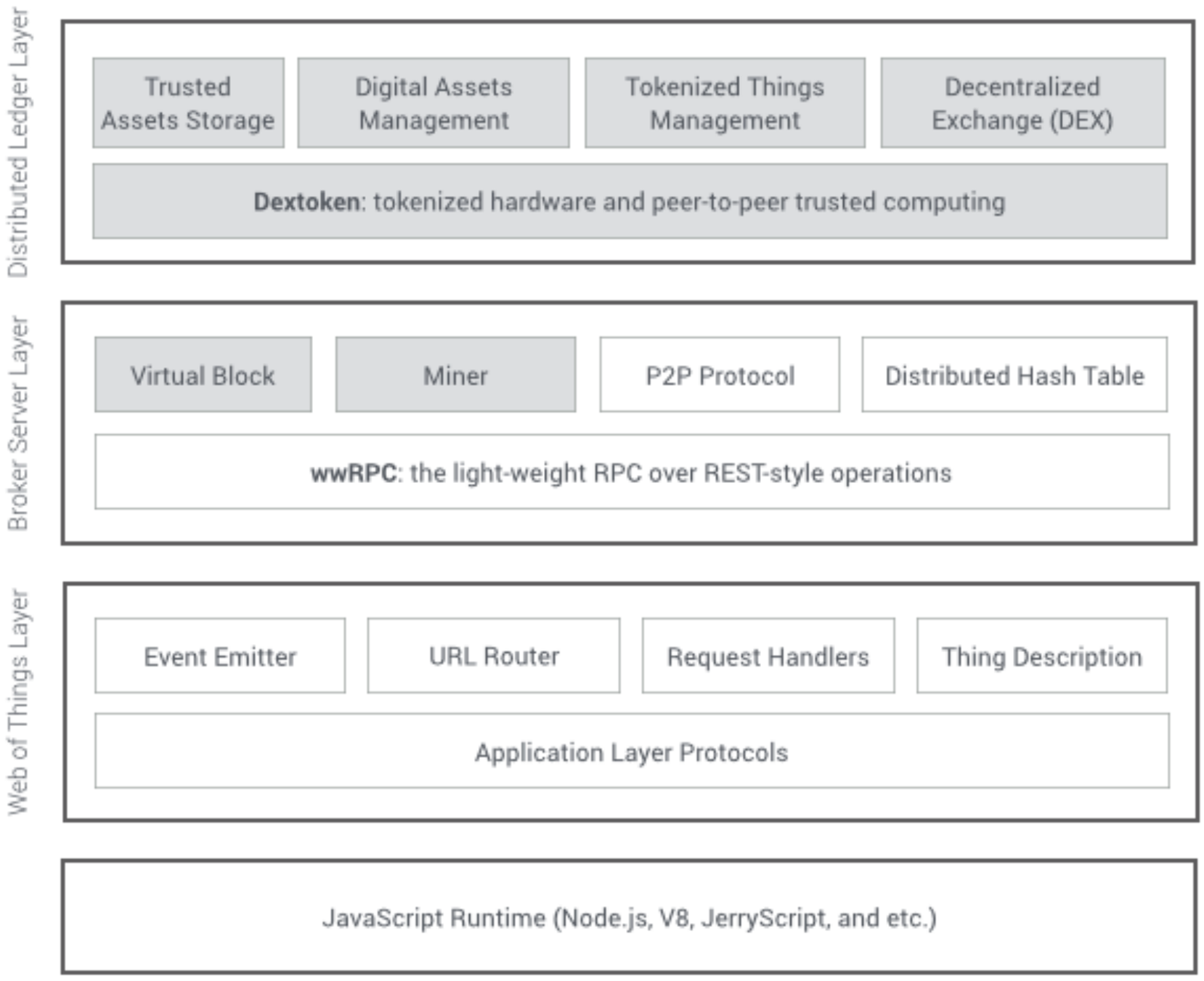


P2P (Distributed)

FLOWCHAIN

Blockchain OS, #2 of 4

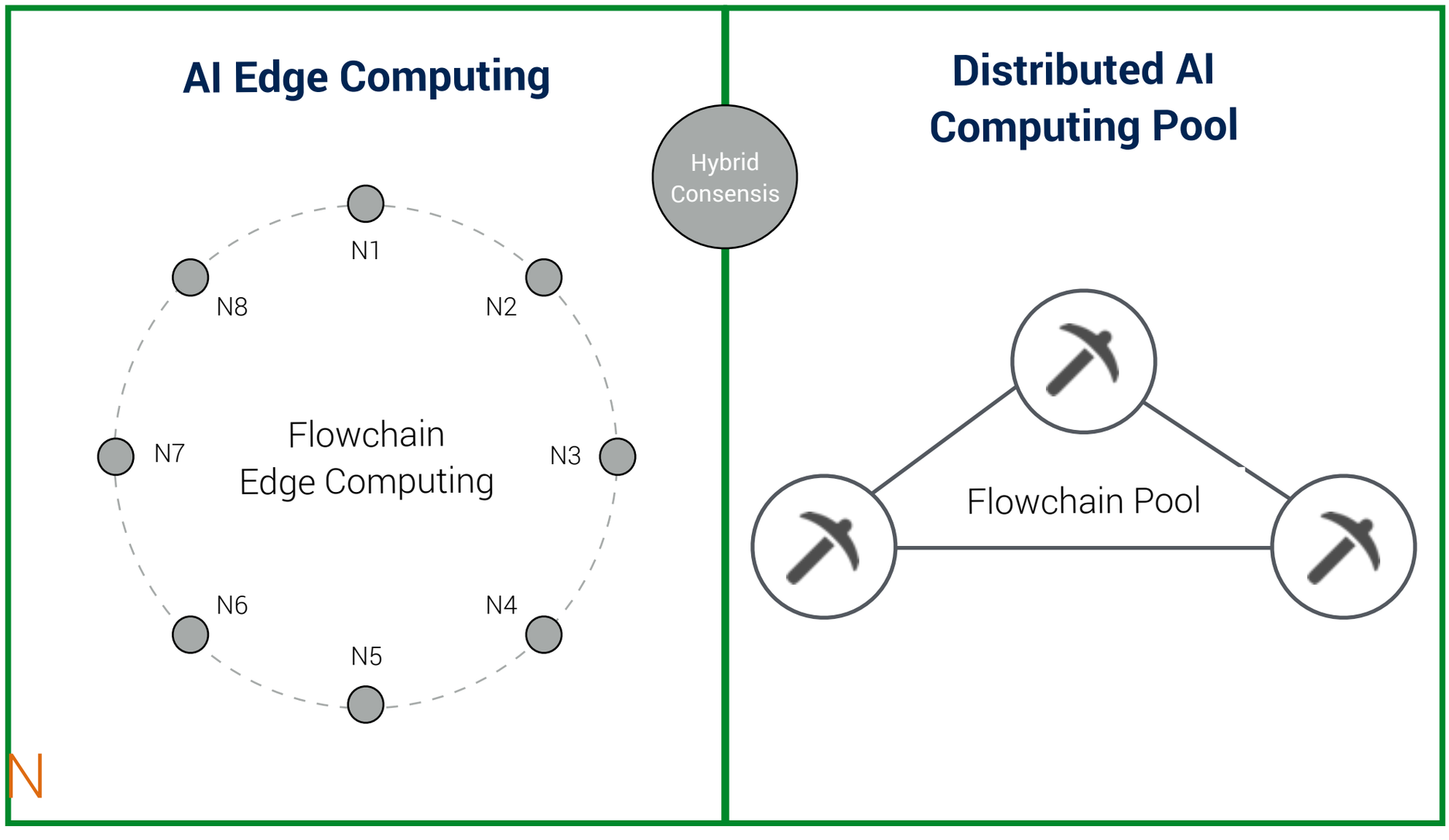
- The flowchain OS enables Device Autonomous Machines



FLOWCHAIN

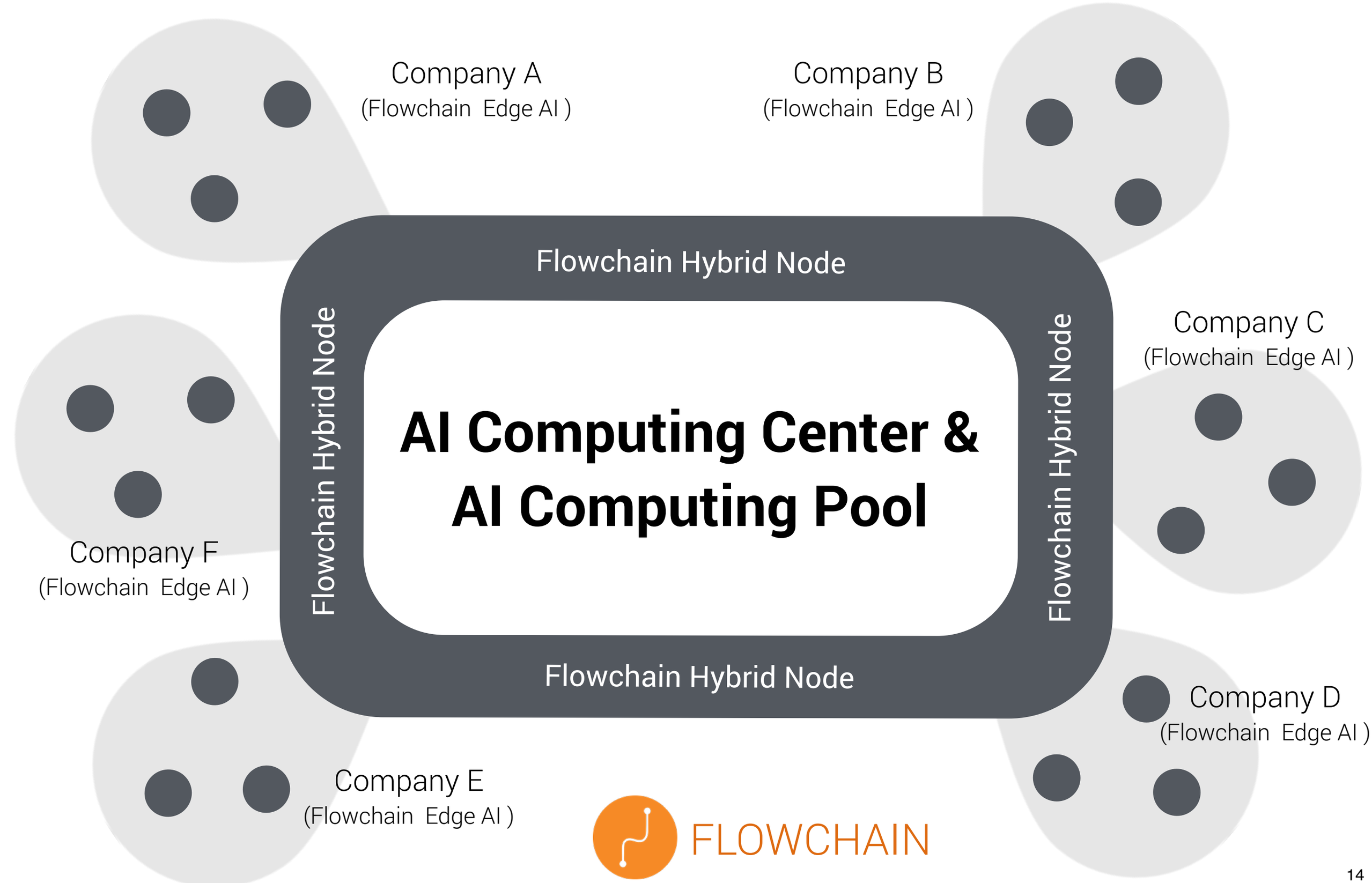
Hybrid Blockchain, #3 of 4

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



FLOWCHAIN

Decentralized AI, #4 of 4



Flowchain

Hybrid

Blockchain

Public Blockchains

Anyone can join the blockchain network that the blockchain network is completely open to users for submitting transactions.

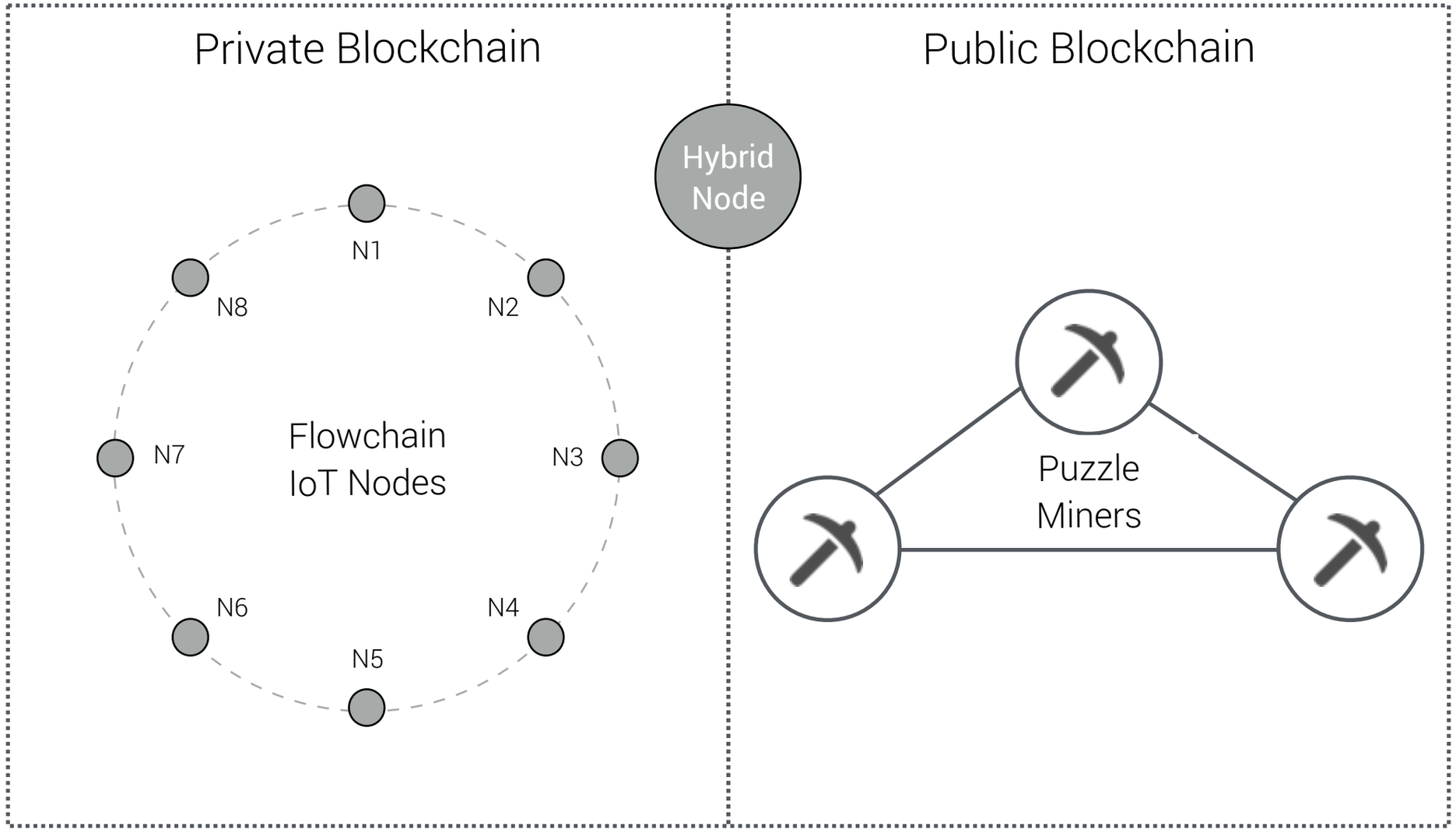
The public blockchain can enable a decentralized model that it can operate without any central authorizations; thus the public blockchain has the natures of *openness* and *trust.*

Private Blockchains

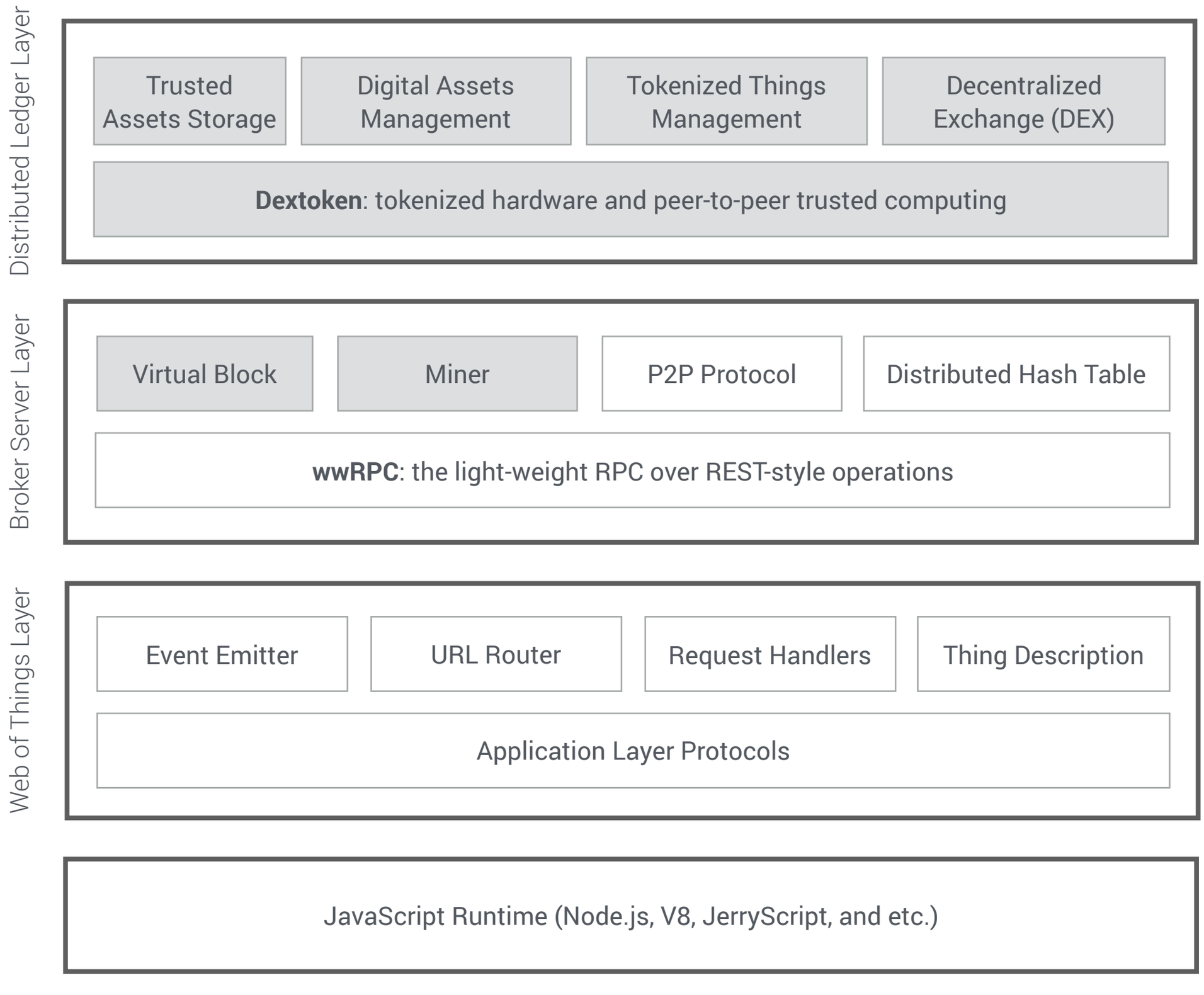
Only authenticated users can join the private blockchain network.

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)**



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

Flowchain OS runs **Everywhere**

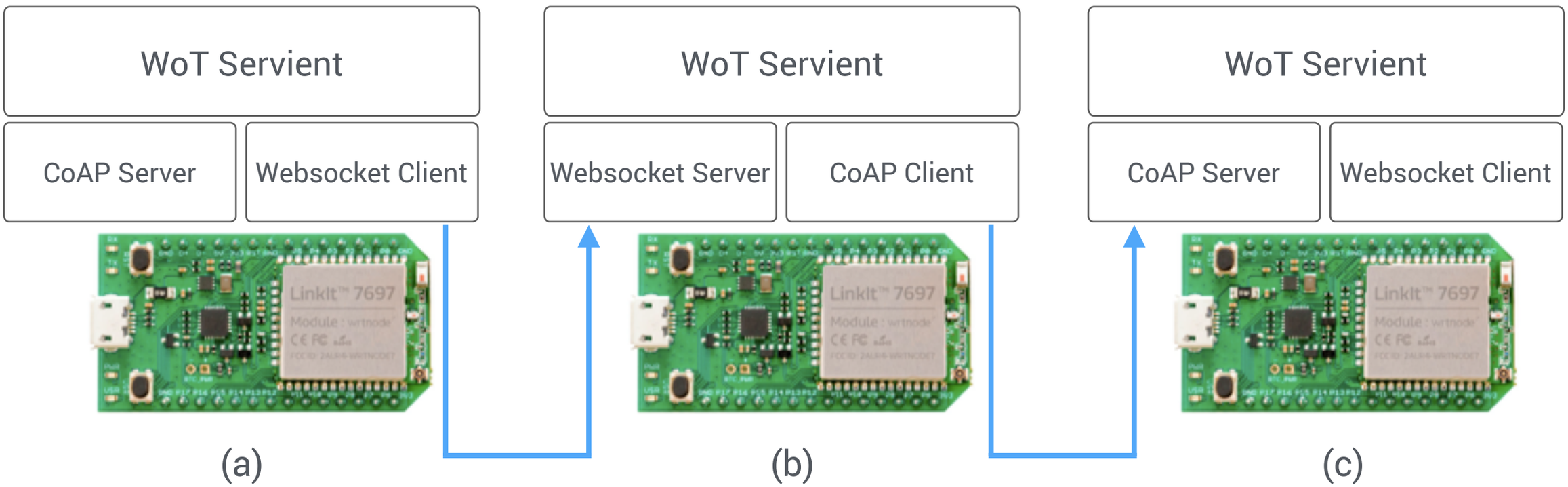
Dapps	Dapps	Dapps	JavaScript
RPC & DHT	RPC & DHT	RPC & DHT	JavaScript
Thing (WoT)	Thing (WoT)	Thing (WoT)	JavaScript
WebSocket / CoAP	WebSocket / CoAP	WebSocket / CoAP	JavaScript
Node.js 0.12	JerryScript	Node.js 4.4+	
OpenWRT (Linux)	FreeRTOS	MacOS	
MIPS Processor	ARM Cortex-M4	Intel Core 2	
580MHz 128MB DDR2 32MB Flash	192MHz 352KB RAM 4MB Flash	1.4GHz 2GB DDR3 64GB SSD	

heterogeneous Hardware

FLOWCHAIN

The Broker Server Layer

- A WoT Servient comprises of client and server combinations.



FLOWCHAIN

Flowchain

Algorithms

P2P Geography over Chord

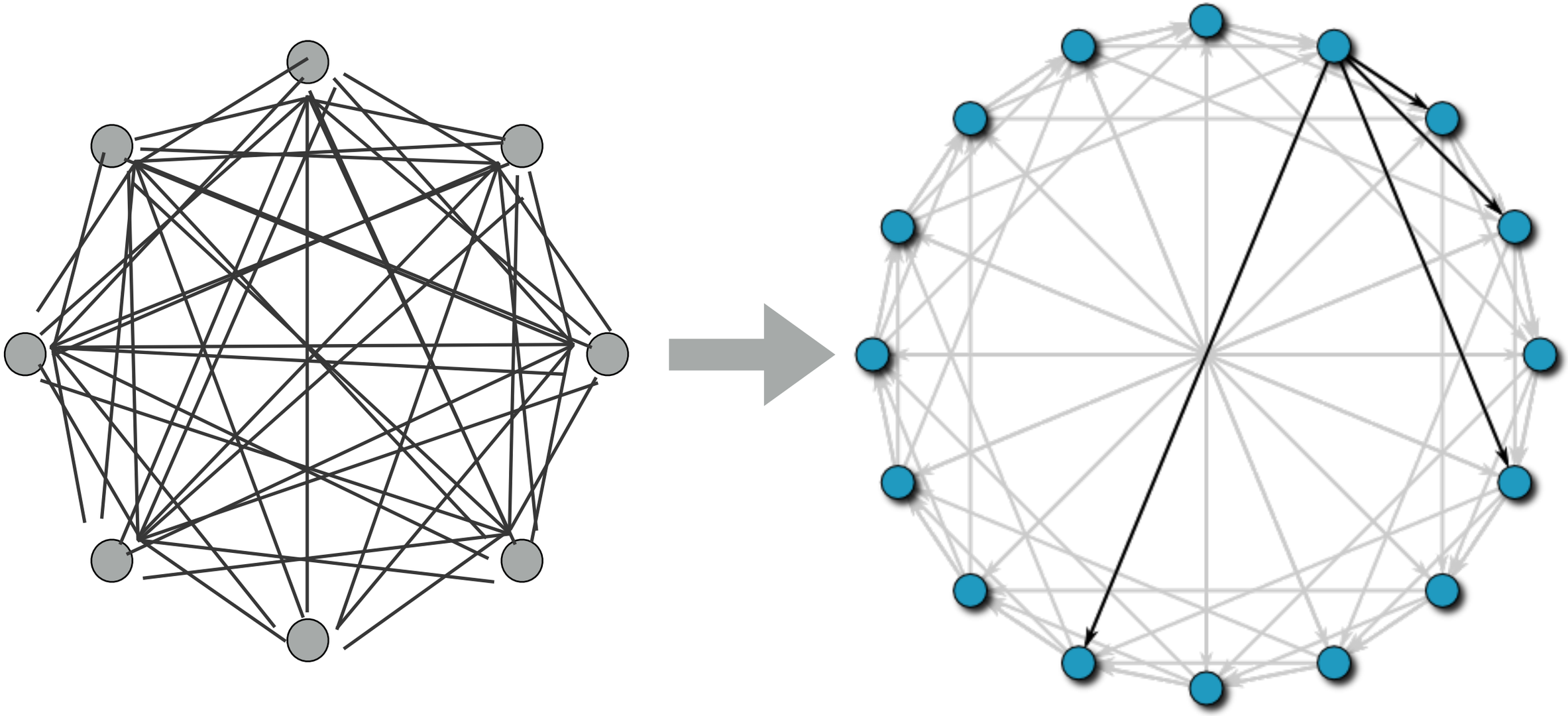
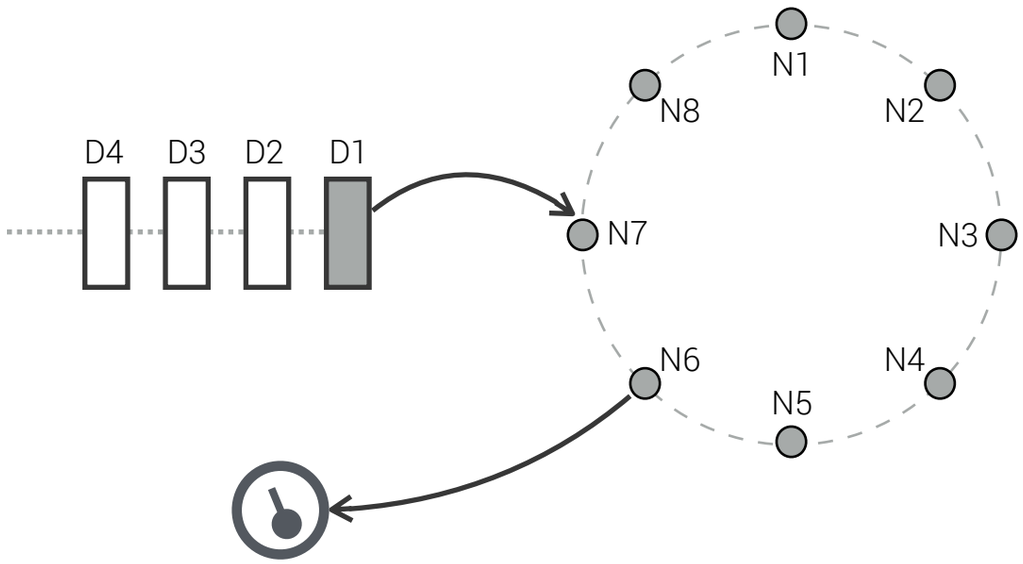


Figure: A 16-node Chord network. The "fingers" for one of the nodes are highlighted. License: CC BY-SA 3.0. Source: https://en.wikipedia.org/wiki/Chord_(peer-to-peer)

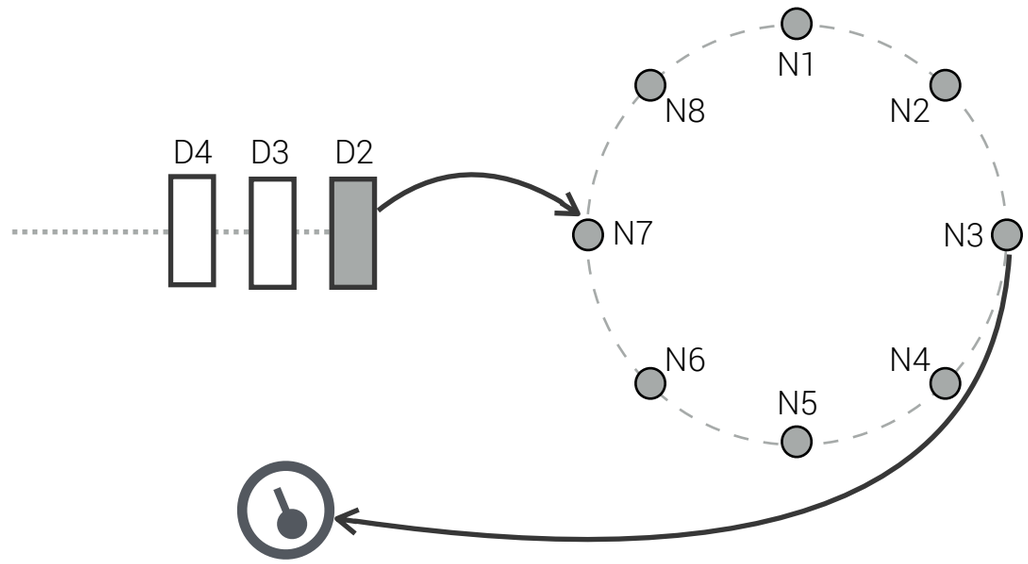
FLOWCHAIN

SUCCESSOR(D1) = N6



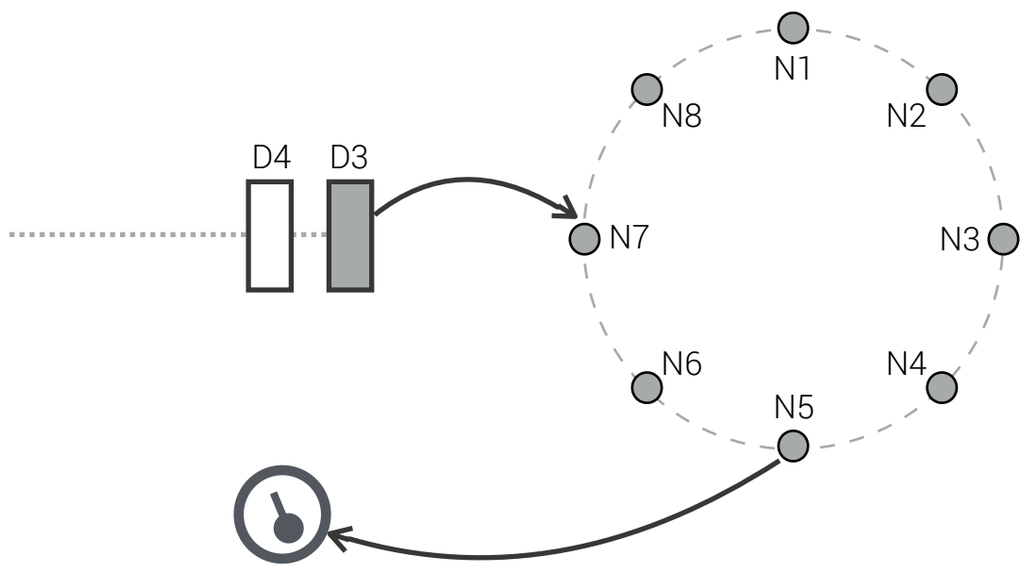
(a)

SUCCESSOR(D2) = N3



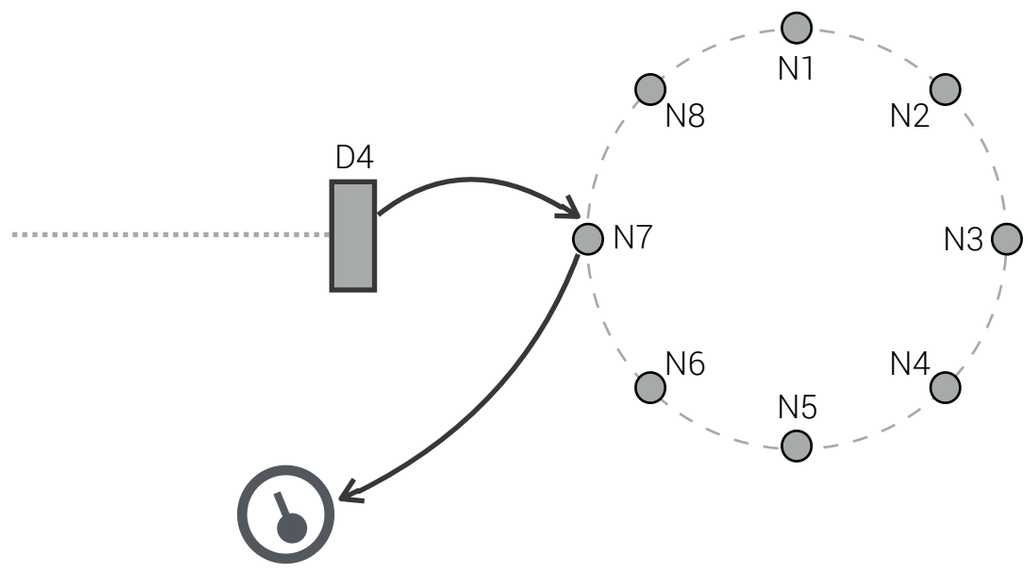
(b)

SUCCESSOR(D3) = N5



(c)

SUCCESSOR(D4) = N7



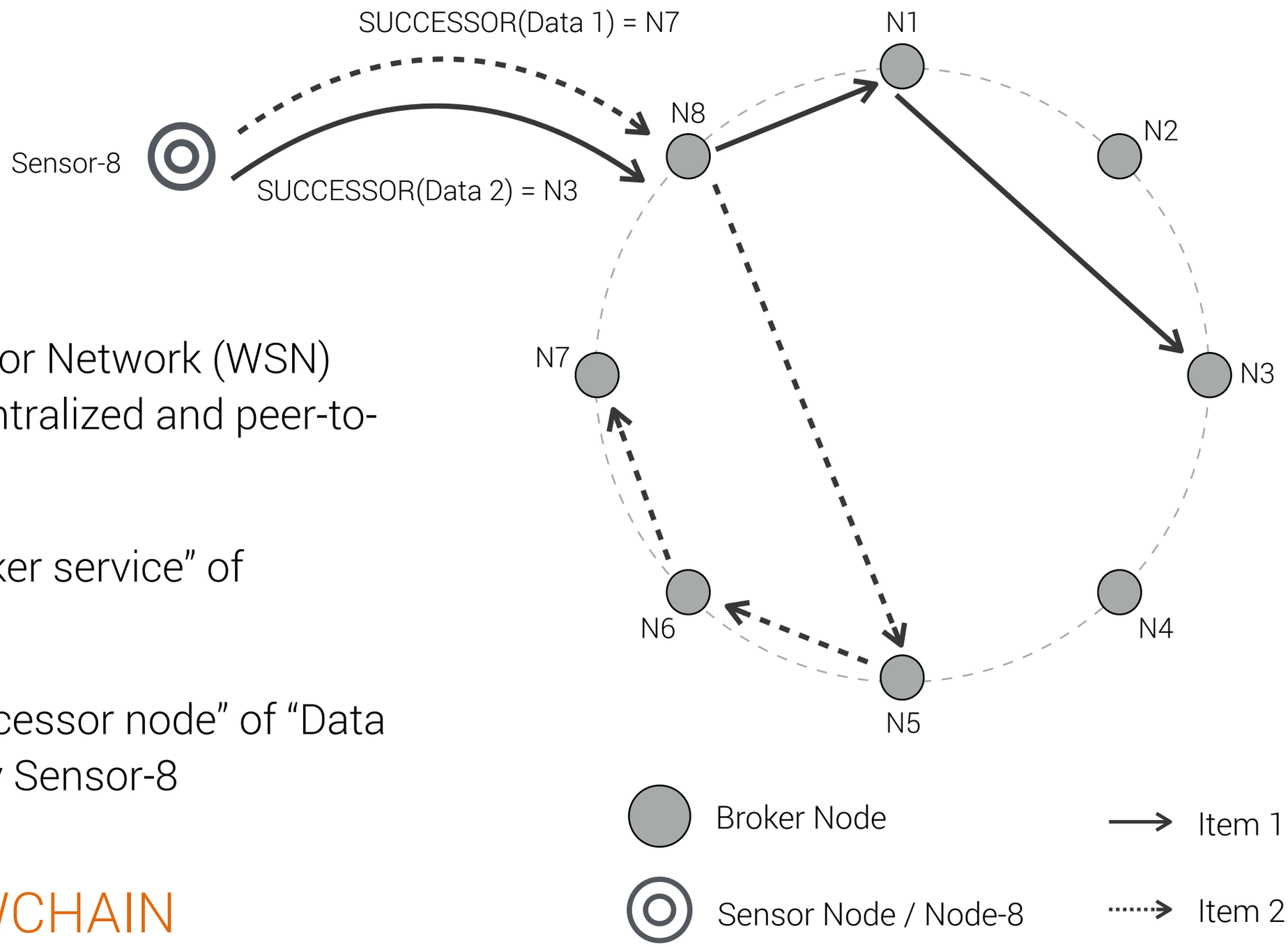
(d)

Flowchain Node

Endpoint Node

FLOWCHAIN

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

FLOWCHAIN

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

FLOWCHAIN

Generating Transaction ID

- Use SHA256, SHA1, and Double SHA256
- The **H**DATA hash is generated by the p2p network

$$H_{BLOCK} = \mathbf{SHA256(}\ BlockNo + timestamp + nonce\ \mathbf{)}$$
$$H_{DATA} = \mathbf{SHA1(}\ data + timestamp + Konami\ Code\ \mathbf{)}$$

$$H_{txID} = \mathbf{SHA256(\ SHA256(}\ H_{BLOCK} + H_{DATA}\ \mathbf{)\ )}$$

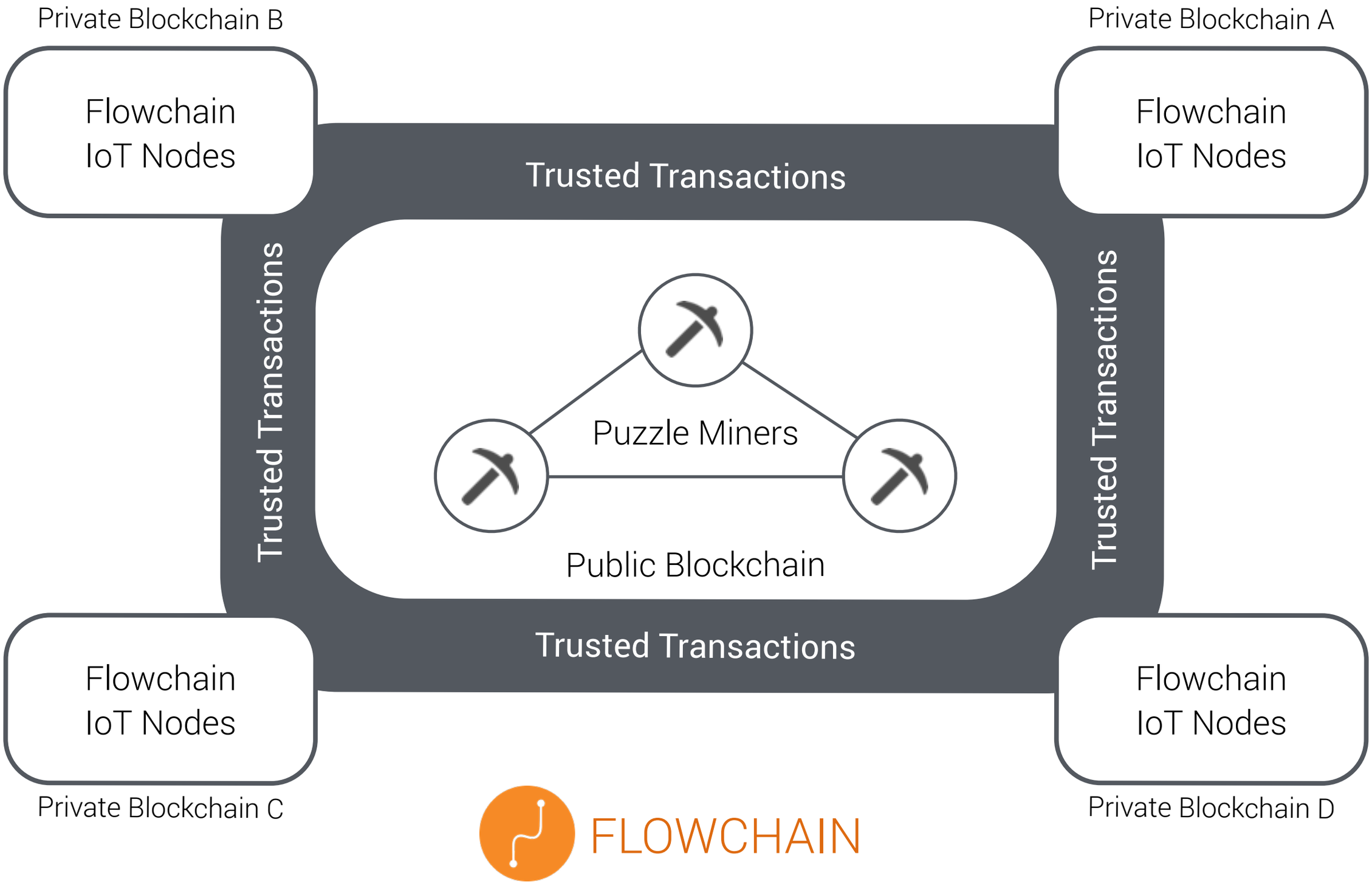
FLOWCHAIN

Data Transactions

- **The data transaction process**
  - Step 1: Generate the key of the data - $\mathbf{H}_{DATA}$
  - Step 2: Search the successor node of the key in the DHT - SUCCESSOR($\mathbf{H}_{DATA}$)
  - Step 3: Send [$\mathbf{H}_{DATA}$, Konami Code] to the successor node over the RPC operations
  - Step 4: The successor node generates $\mathbf{H}_{txID}$
  - Step 5: The successor node signs (optional) and submits H_{txID} to the public blockchain

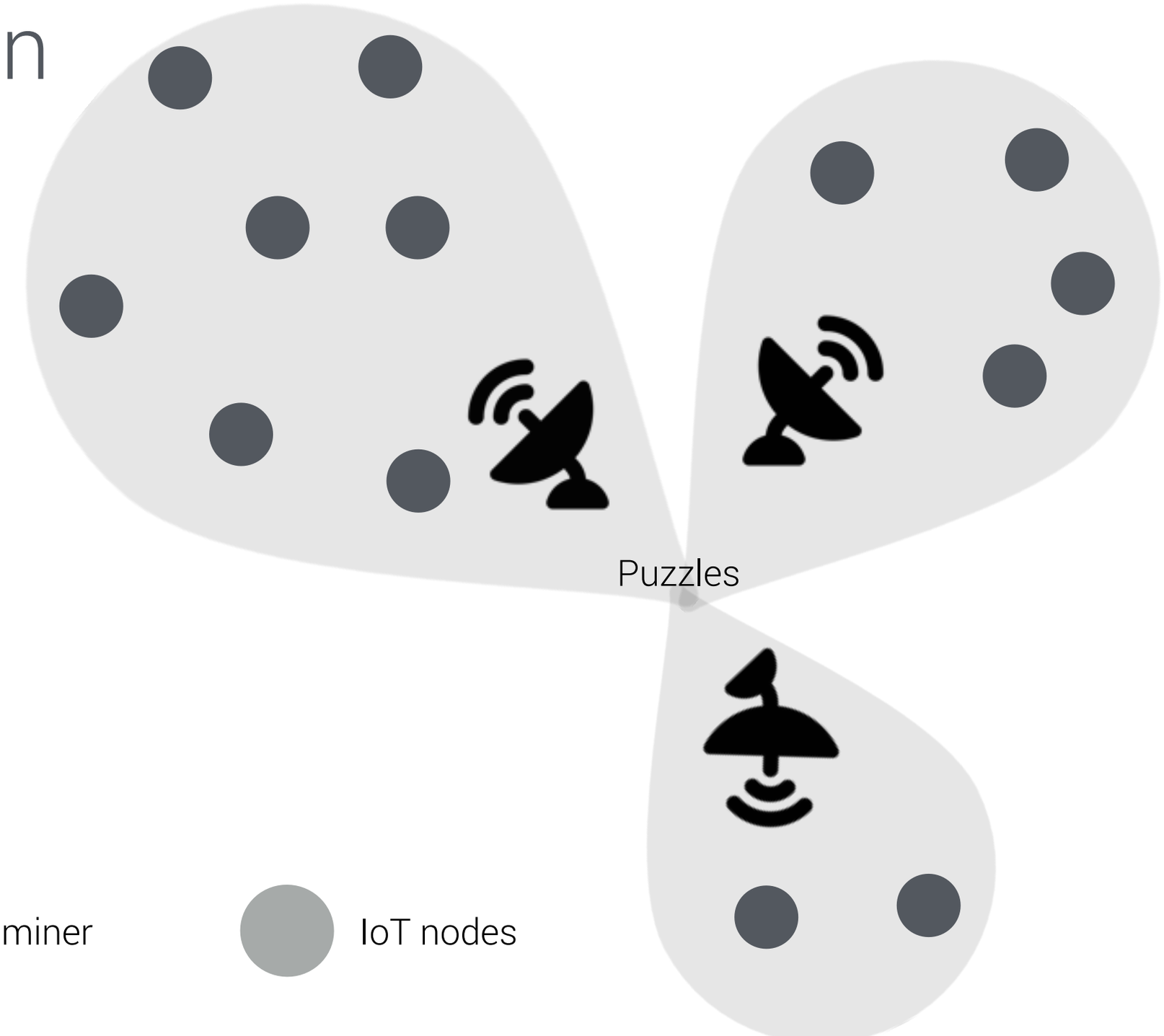
FLOWCHAIN

Hybrid Flowchain: IoT Blockchain + AI over **Pseudonymous Authentication**



FLOWCHAIN

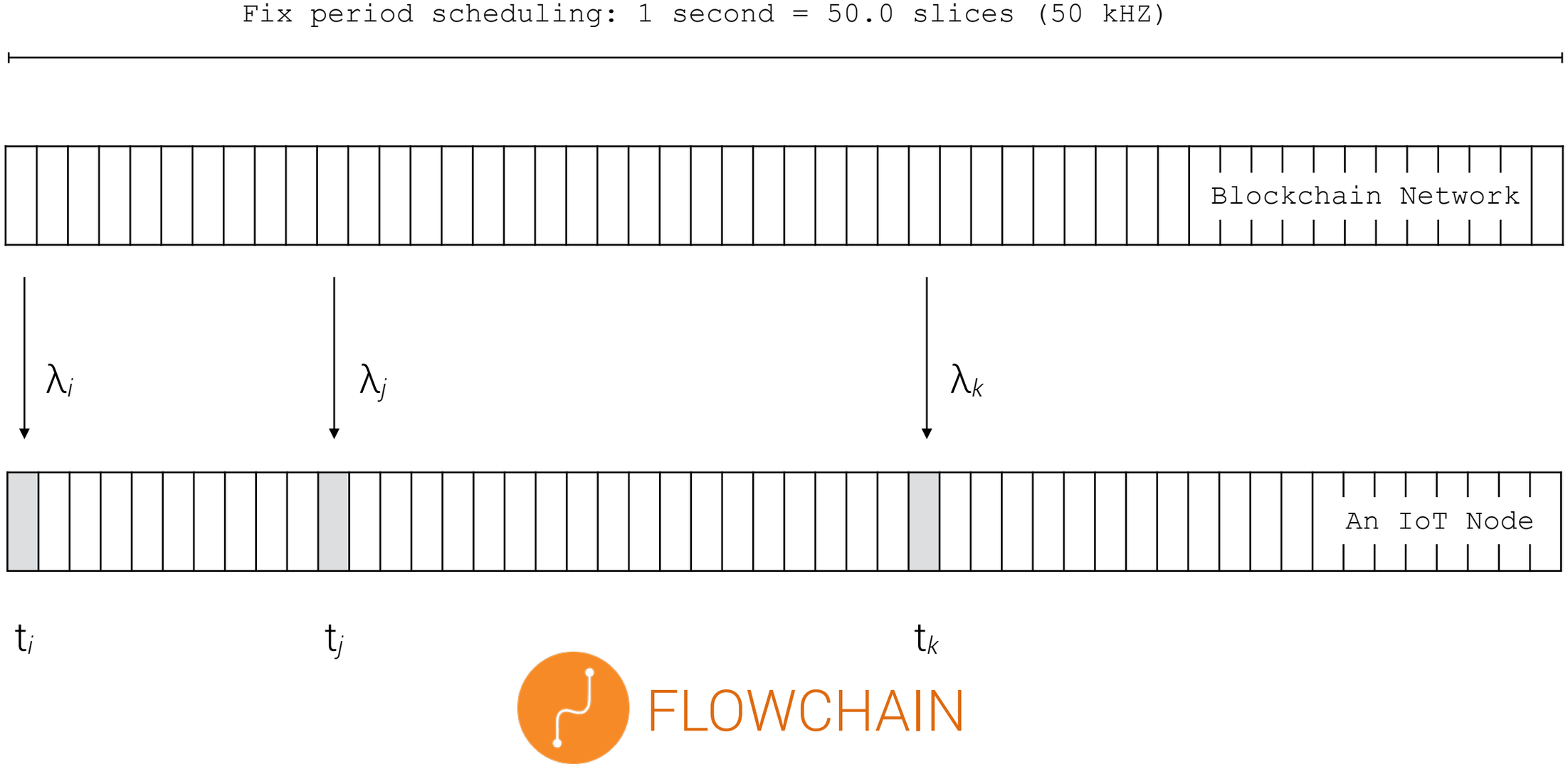
Pseudonymous authentication can replace the PKI to enable a fast authentication



FLOWCHAIN

Puzzle Miner is a scheduler that provides time-difficulty string search puzzles

The IoT node was pseudonymously authenticated to submit transactions at (ti,tj,tk).



FLOWCHAIN

Puzzle Miner algorithm

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

Jollen Chen
Devify Open Source Project
Devify, Inc.
jollen@flowchain.io

ABSTRACT

Keywords

I. INTRODUCTION

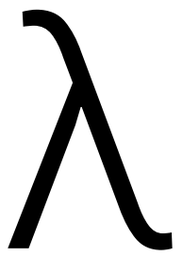
II. MOTIVATION

Figure 1: The Devify Architectural Design

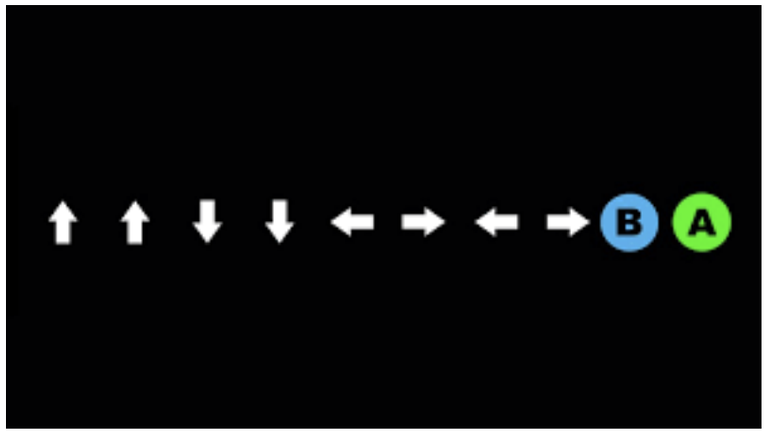
Hybrid Flowchain: Smart Contract Platform for Distributed Autonomous Machines

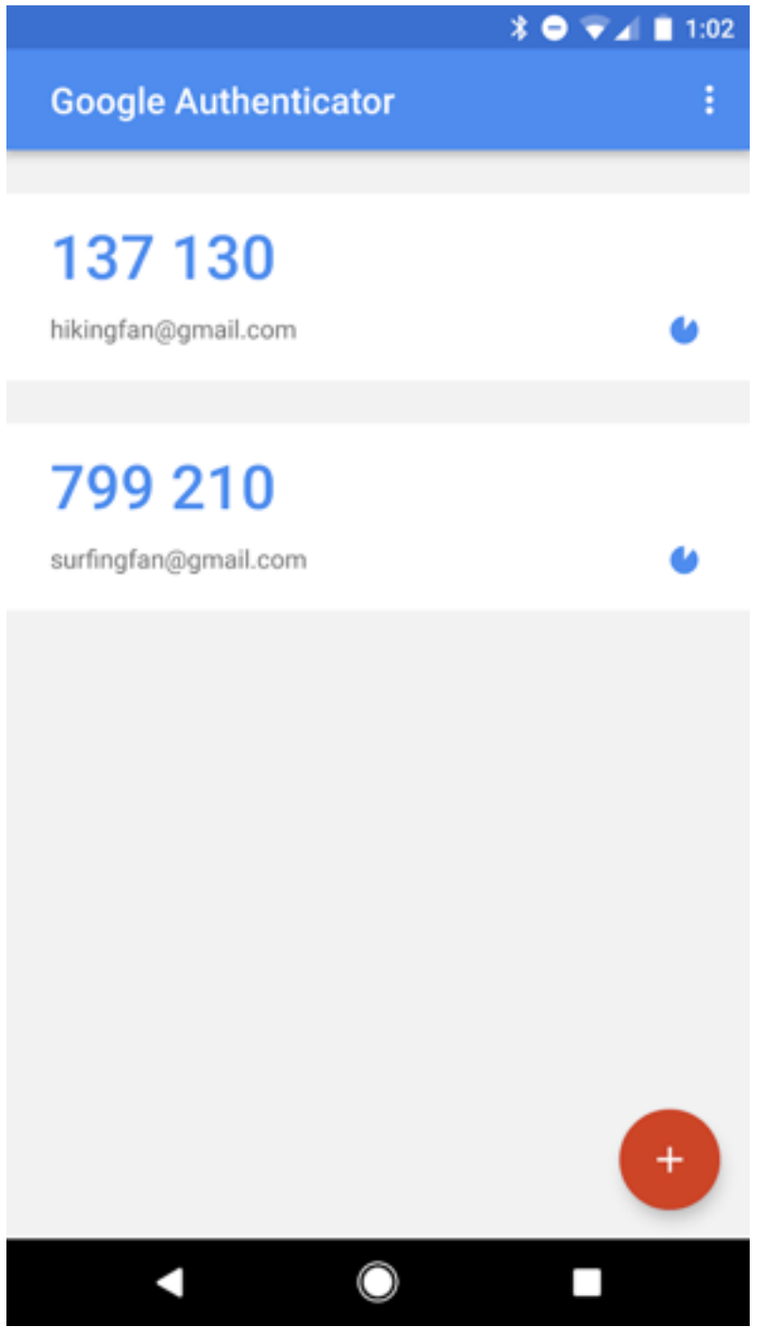
1. $\mathcal{U}i$ starts receiving λ from the broadcasting
2. Let $\mathcal{P}uzzle$ be a function and $\S_j$ be a string; $\mathcal{U}i$ receives a puzzle $(\mathcal{P}uzzle, x_j)$ from a peer $\mathcal{U}j$ in the private blockchain over the p2p network
3. Let $\mathcal{P}uzzle(\lambda)$ gives an arbitrary-length 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 $\mathcal{U}i$ solves the puzzle $(\mathcal{P}uzzle, x_j)$ if $\mathcal{F}puz$ successfully finds $y_i = x_j$ within the time interval σ
6. $\mathcal{F}puz$ returns $\S_j$ to $\mathcal{U}j$ and stores $\mathcal{H} = (\vec{x}, y_i, \lambda)$ in $\mathcal{T}$
7. The miners and $\mathcal{U}j$ confirm the user $\mathcal{U}i$ is *authenticated*

FLOWCHAIN



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 $\mathcal{U}i$ produces a message or receives a message from another user through the p2p network; formally, let $\mathcal{M}$ be this message
2. The trusted user $\mathcal{U}i$ has the keypair (sk_i, pi_i); let $\mathcal{S}ign$ be the signature function
3. Let $\mathcal{T}i$ be the new transaction and $\mathcal{H}ash$ be a hash function so that $\mathcal{T}i = \mathcal{H}ash(\mathcal{S}ign(M), H, pk_i)$;
4. $\mathcal{U}i$ submits $\mathcal{T}i$ to the public blockchain

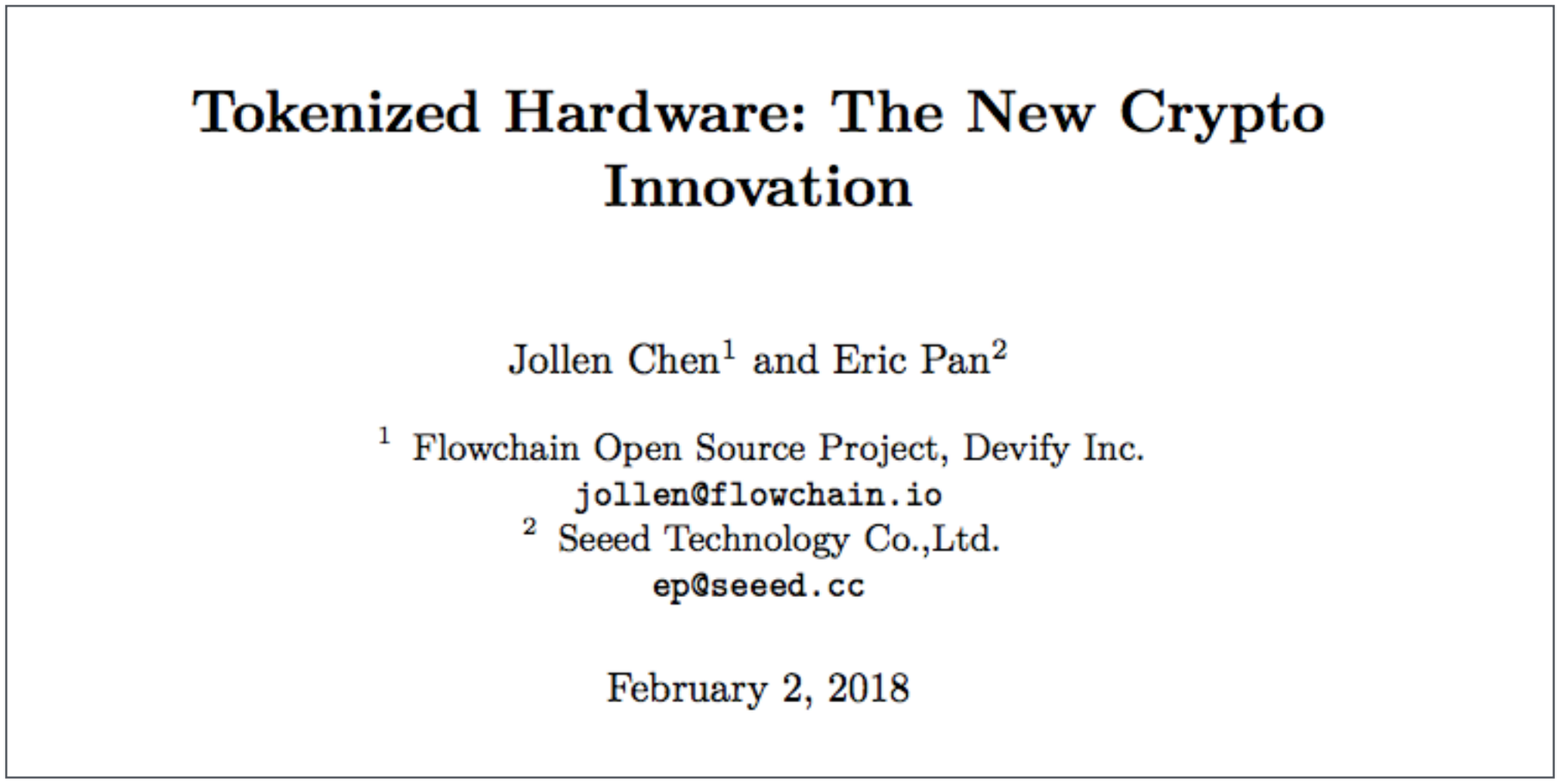
FLOWCHAIN

Flowchain

Tokenized

Hardware

Cooperate on Tokenized Hardware



Tokenized Hardware: The New Crypto Innovation

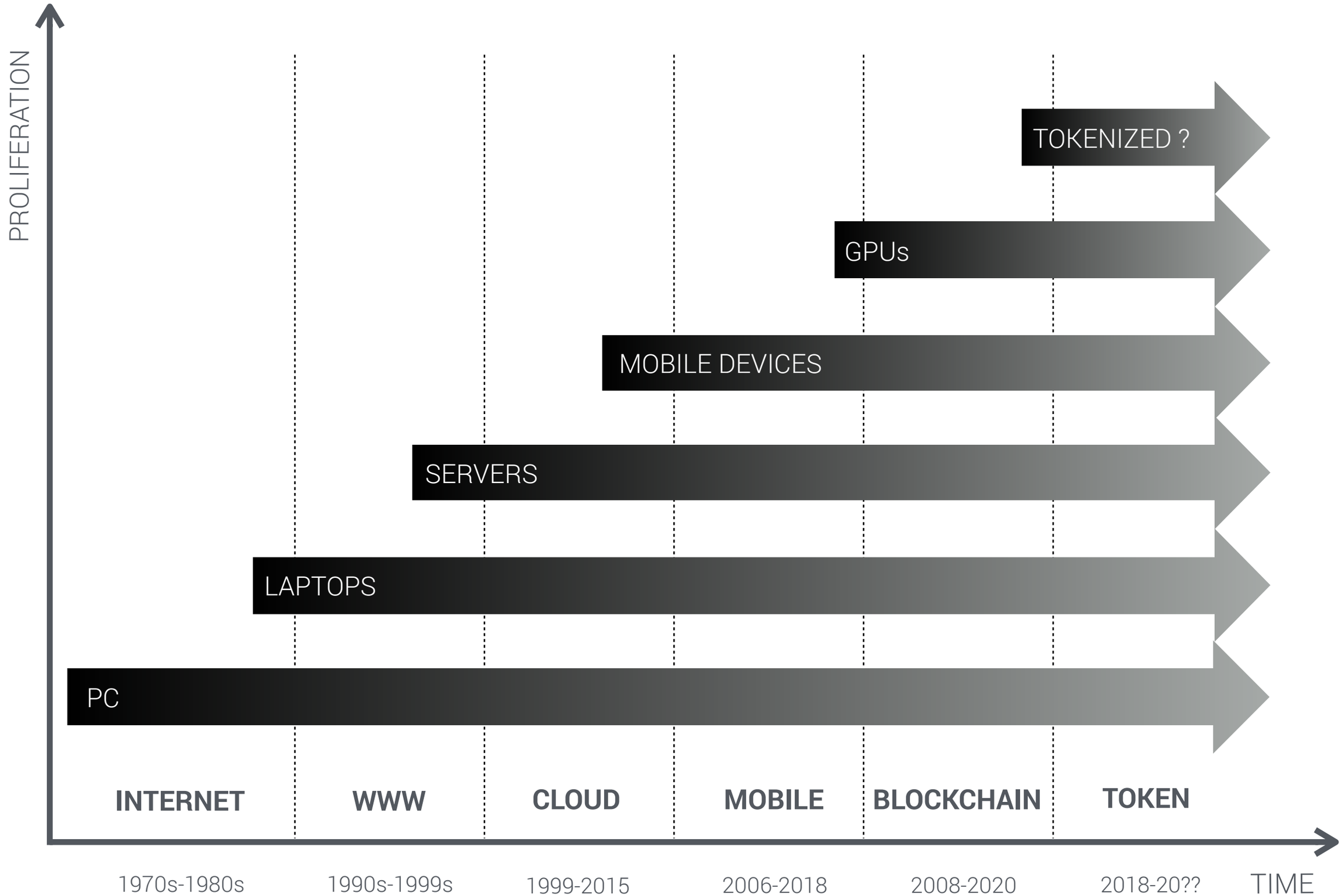
Jollen Chen[1] and Eric Pan[2]

[1] Flowchain Open Source Project, Devify Inc.
jollen@flowchain.io
[2] Seeed Technology Co.,Ltd.
ep@seeed.cc

February 2, 2018

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.


PROLIFERATION
TOKENIZED ?
GPUs
MOBILE DEVICES
SERVERS
LAPTOPS
PC
INTERNET
WWW
CLOUD
MOBILE
BLOCKCHAIN
TOKEN
1970s-1980s
1990s-1999s
1999-2015
2006-2018
2008-2020
2018-20??
TIME

FLOWCHAIN

From Hardware to Tokenized Hardware

Hardware	v.s.	Tokenized Hardware
• Tangible assets		• Tangible assets • Digital assets • Ownership • Rights • Depreciation • Externality • Decentralized assets Exchange (Dextoken)

FlowchainCoin (FLC) is an utility token that can be used in tokenizing hardware and accessing the Flowchain platform.

FLOWCHAIN

Conclusions

How can apps trust the data sent from an arbitrary device ?

Decentralized is impossible if we have to use trusted thirty parties.

FLOWCHAIN

Trusted thirty parties removed by Flowchain using the blockchain technologies

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

FLOWCHAIN

The Flowchain Model

The AI Dapps

Distributed Autonomous Machines

Trustless Communication and Consensus

Trusted Hardware

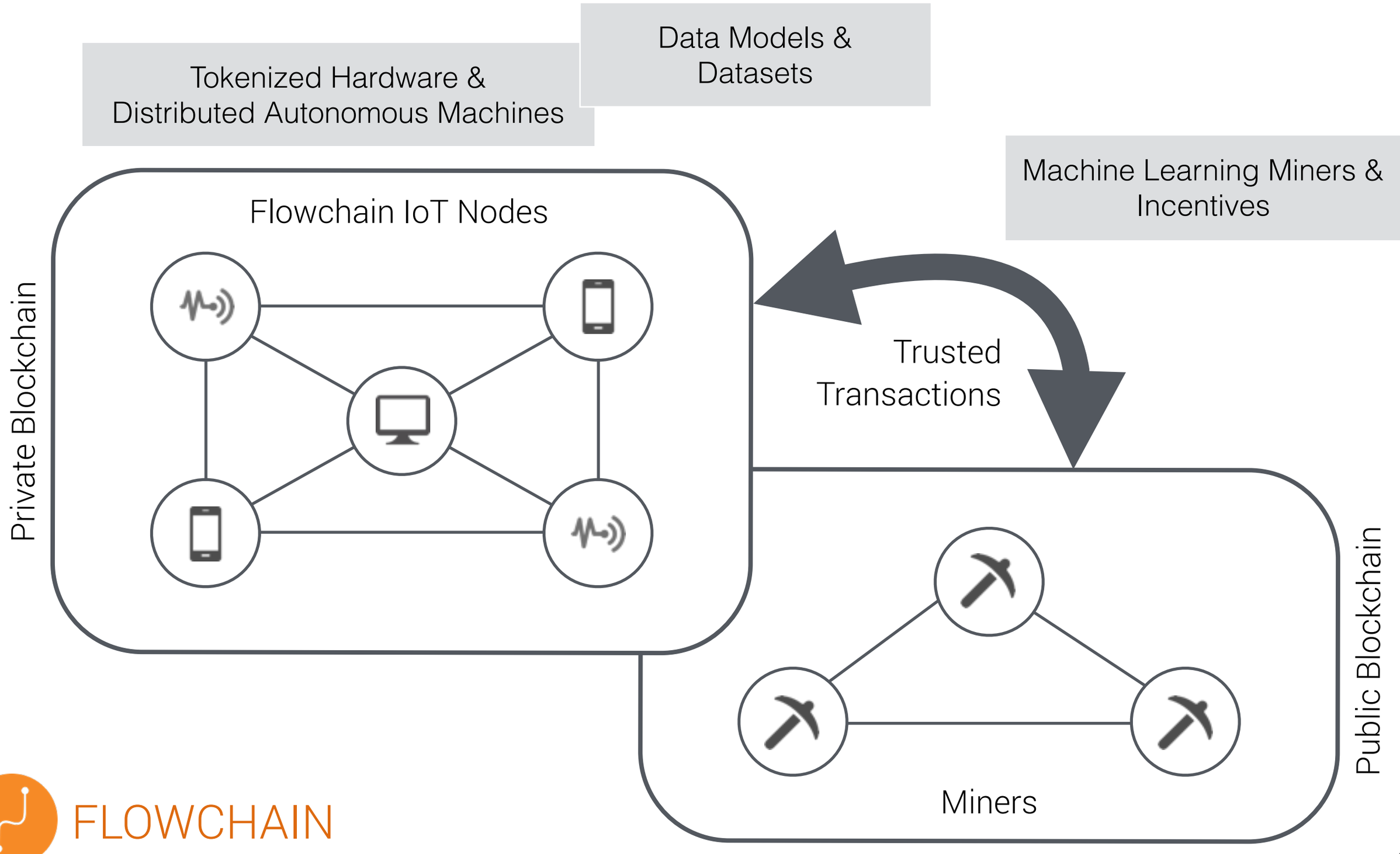
FLOWCHAIN

Flowchain underlying layer: Tokenized Hardware + DAM

	Current Trusted Computing Model	Flowchain Trustless Computing Model
Secure input and output	ARM TrustZone Virtualization Linux	Tokenized & Trusted Hardware
Memory curtaining / protected execution		
Endorsement key	Cryptography	Distributed Autonomous Machines
Sealed storage	DRM	
Remote attestation	CA PKI HMAC	
Trusted Third Party (TTP)		

FLOWCHAIN

Flowchain uppermost layer: AI over IoT Blockchain



FLOWCHAIN

FLOWCHAIN

Website **https://flowchain.co**

Github **https://github.com/flowchain**

Contact **jollen@flowchain.io**

WeChat **jollentw**