



**THINK OPEN**

开放性思维

# A Hybrid Blockchain for the IoT and Tokenized Hardware

Jollen Chen, Founder & CEO, Flowchain

Beijing, China, June, 26, 2018

LF ASIA, LLC



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>.

# **Flowchain**

## Quick Start

# Flowchain Visions



$$\text{Flowchain} = (\text{mining}) * (\text{IoT, Blockchain, AI})$$



Cryptocurrency  
(Incentives)



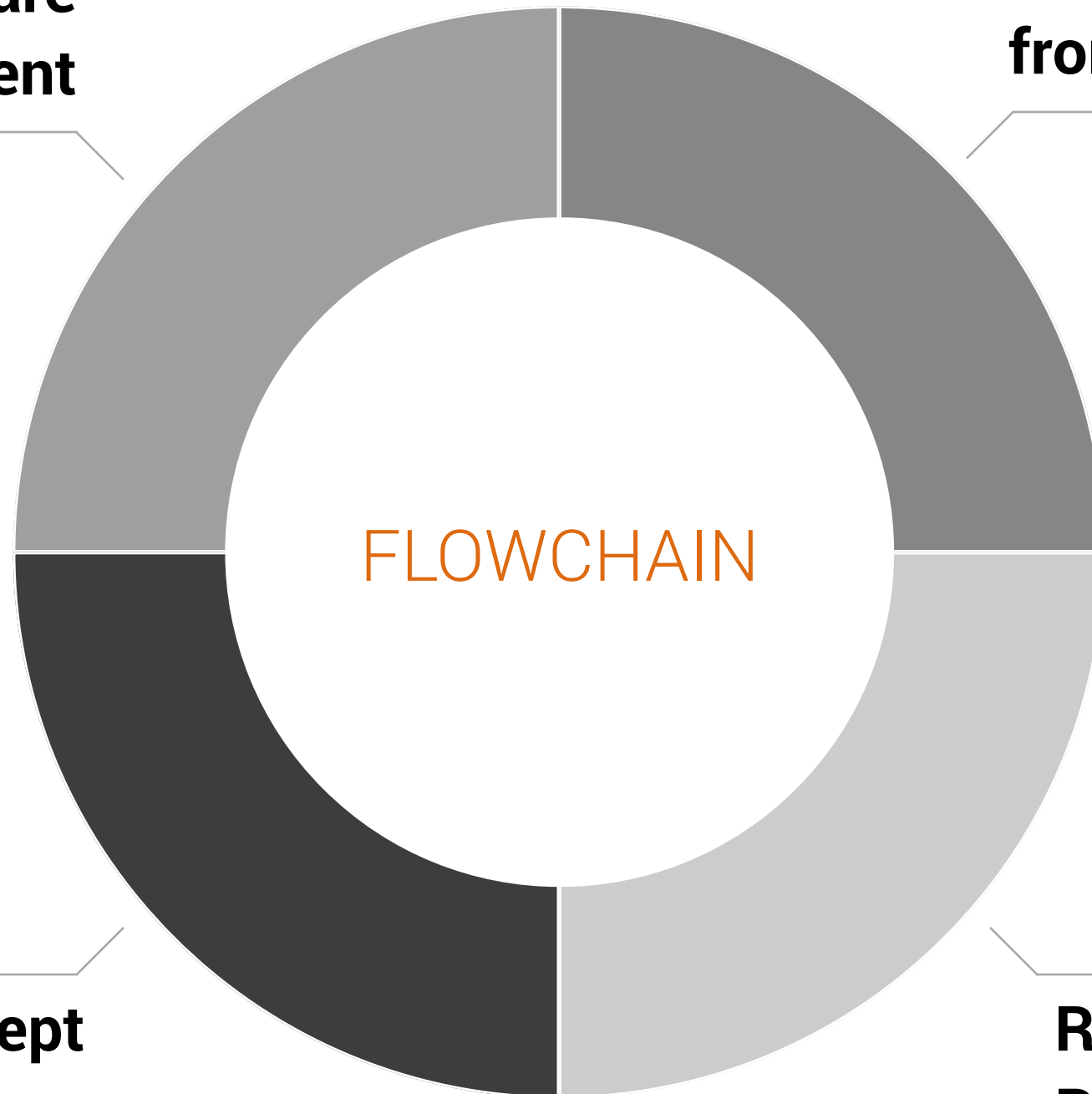
Flowchain Technologies

# 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

# Github Repositories




## Flowchain

A distributed ledger for the Internet-of-Things (aka. IoT Blockchain) in JavaScript

<https://flowchain.co/> [jollen@flowchain.io](mailto: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

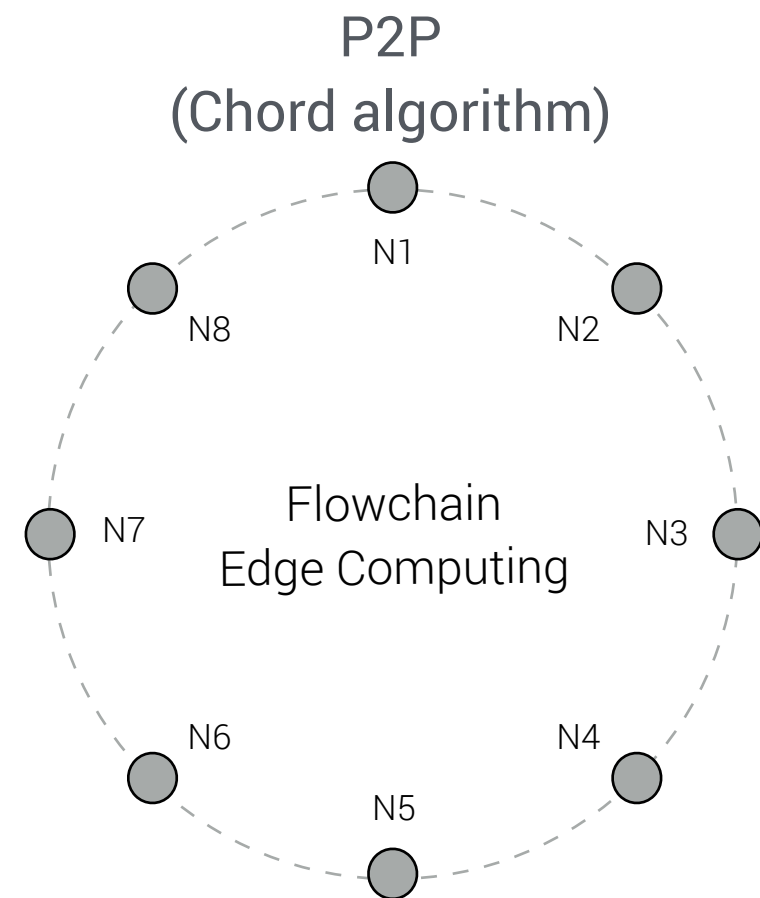
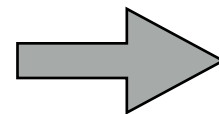
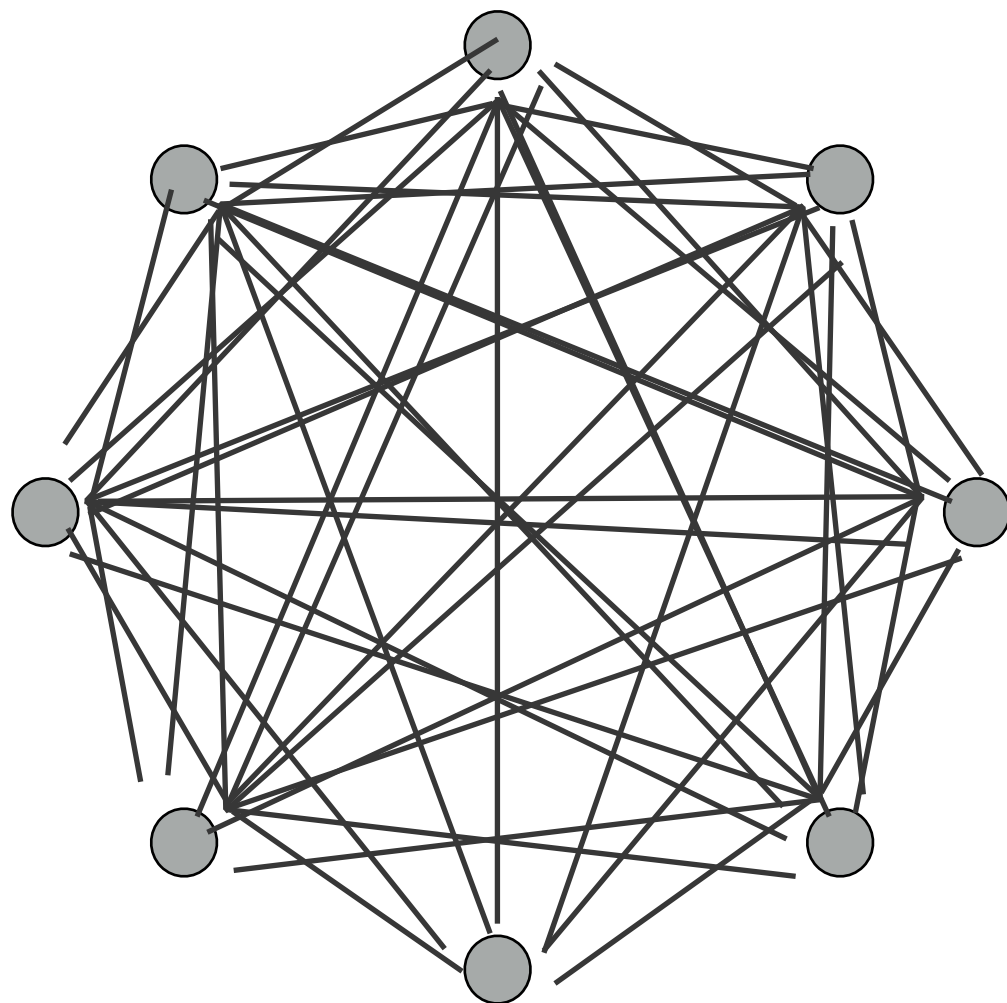
- The data **flow** block**chain**
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI



# Dataflow Blockchain, #1 of 4



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



# Academic Papers



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

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

### ABSTRACT

This paper addresses the issue of current Internet of Things (IoT) development - the decentralized IoT model - in a manner of a peer-to-peer network and interoperable IoT device. This paper proposes a new IoT software architecture, the Devify software framework, to address the peer-to-peer IoT network and the interoperable IoT device development. Besides, the work also shows through experiments that an IoT application server can simply use the flow-based programming (FBP) paradigm to define the application as a data exchange network. Therefore, the software architecture also provides such FBP runtime environments for writing IoT applications server.

### Keywords

Internet of Things, Interoperability, Peer-to-Peer, Web of Things, Decentralized, Flow-Based Programming

### 1. INTRODUCTION

In recent years, the development of Internet of Things (IoT) applications has become increasingly complex. Thus, many studies have attempted to address the problem by providing the ability to access IoT data to the IoT platform over the web to simplify the creation of IoT applications [1]. However, current existing IoT platforms are the centralized model that they act as brokers or hubs to control the exchanged data between IoT devices. Therefore, many studies expect that IoT should use the decentralized model to ensure secure data exchange and data privacy. Thus, this paper proposes a decentralized IoT software framework to provide the ability of secure data exchange between IoT device autonomously without any centralized server. In short, the purpose of a new design for the IoT software architecture is that we need a *devify* programming framework to support each full range hardware devices. Besides, the Devify software framework implements the requirements of emerging IoT trends: (1) the peer-to-peer networking for IoT devices, (2) a full stack devify software framework, (3) the device interoperability via REST-style HTTP operations, and (4) the use of the Web of Things (WoT) and JSON-LD ontology.

The rest of this paper is organized as follows: we describe the motivation of this work in Section 2, and subsequently



Figure 1: The Devify Architectural Design

study the related work in Section 3. In Section 4, we introduce the proposed software framework and review what technologies are adopted in the software framework. In Section 5, we review the design and implementation details of the peer-to-peer network as well as the way to address the problem of access in peer-to-peer network. In Section 6, we propose the use of the flow-based programming (FBP) paradigm to create the IoT application server. In Section 7, we show two Devify application examples. We conclude in Section 8.

### 2. MOTIVATION

The motivation of this paper is to develop a generic and comprehensive software framework for building various types of new IoT networks in a decentralized manner. Also, current IoT network comprises a variety range of hardware devices, such as cloud servers, mobile devices, and resource-constrained devices (like heterogeneous IoT hardware devices). Thus, the software framework must be able to monitor on all these hardware devices. Since the blockchain has become a significant technology in the proximity of IoT hardware devices, this paper proposes a REST-like devify programming framework for the software framework to support each IoT hardware.

Furthermore, the motivation of the decentralized IoT should address the device interoperability and a peer-to-peer network, thus, this paper will also address such technical challenges. In this work, we attempt to build a generic software framework for future developments of decentralized IoT applications. Among the potential decentralized IoT applications, the nature of the distributed ledger technology (DLT) has a huge opportunity to build a new type of peer-to-peer IoT network. Therefore, we have already developed Flowchain [2], the blockchain for the IoT, to practically prove the concept of this work.

Copyright retained by the authors.

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.*

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

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

**Abstract.** Recently, the blockchain for the IoT has combined an emerging technology for creating secure access and secure non-repudiable IoT systems. Despite a great of studies on blockchain IoT, few studies have investigated how an IoT blockchain system works in practice. In this paper, we propose Flowchain, an open source distributed ledger programming framework for peer-to-peer IoT networks and real-time data transactions. The main feature of the Flowchain framework is Virtual Blocks that provides a new blockchain data structure design to ensure the real-time data transactions. This paper also propose a software architecture that provides peer-to-peer IoT networking and interoperable IoT application framework.

**Keywords:** Blockchain, Distributed Ledger, IoT, P2P, WoT, JSON-LD

### 1. Introduction

Blockchain, a frequently referenced terminology, uses a distributed database system called a blockchain [3]. The Bitcoin blockchain can operate without any central server that the transactions stand with high trust. Although the Bitcoin blockchain has such decentralized network model, it does not meet the need of current IoT requirements. As the Bitcoin blockchain uses "mined proof" to create new transactions, the average waiting time for verifying a transaction could be 10 minutes that not in a real-time manner. Thus, to address this technical challenge, the main aim of the Flowchain programming framework is to provide a *dedicated* blockchain system for the IoT that can process and record transactions in a real-time manner. Flowchain presents a new verification called Virtual Blocks to provide each real-time transactions ability.

Besides, Bitcoin uses a distributed single blockchain model in which all nodes compete to mine new blocks. However, IoT hardware nodes, e.g., resource-constrained devices, mobile devices, and high-performance server nodes that the computing power varies from devices. Thus, consensus-based functions have been proposed to deal with heterogeneous hardware [4]. The mining process

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.*

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

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

### ABSTRACT

This paper addresses the issue of *secure and trusted* Internet of Things (IoT) networks by adopting the emerging blockchain technologies. This paper proposes a new hybrid blockchain technology to address the trusted IoT issues such as trustless communications and decentralized applications. Besides, we also present that the pseudonymous authentication technique can use a puzzle-solving computation to enable trustless communications for the IoT and provide the capabilities of near real-time transactions. In our previous work, we presented a decentralized software framework for the IoT by using a p2p network and the concept of the blockchain. In this paper, we outline the core components of the hybrid blockchain and delve deeper the algorithms of the hybrid consensus to provide the capabilities for our hybrid blockchain technology.

### Keywords

Internet of Things, Blockchain, Hybrid Consensus, Peer-to-Peer, Trustless Computing, Decentralized

### 1. INTRODUCTION

The Internet of Things (IoT) devices can generate and exchange security-critical data over the IoT network. Many IoT networks use the public-key infrastructure (PKI) to authenticate devices and ensure the data security as well as the data privacy. The IoT device has to sign the generated data by a digital public key, and deliver the data to the network for exchanging. However, such authentication method tends to be expensive for an IoT device regarding computing power and energy consumption.

Furthermore, the blockchain technology has the decentralized, secure, and private nature to become a promising idea that can be approaching the next-generation IoT architecture. Therefore, in our previous work, Flowchain and Devify have already been proposed to build a blockchain technology for the IoT device over a p2p network. Therefore, to achieve a secure and *inexpensive* blockchain for the IoT, this paper proposes *Flowchain Hybrid Blockchain* to enable *fast authentication* by eliminating the concept of traditional PKI methods. Furthermore, our work can address the technical challenge of achieving an efficient and secure IoT device to exchange the captured data by the blockchain technology.

Copyright retained by the authors.

The rest of the paper is organized as follows: In Section 2 we describe the main components of the hybrid blockchain design. In Section 3 we present the model including the architecture, algorithms and the hybrid blockchain design. The IoT blockchain economy is discussed in Section 4. Finally, Section 5 concludes the paper.

### 1.1 Previous Works

#### A. Devify

Devify has already proposed a generic and comprehensive software framework for building various types of trust IoT networks in a decentralized manner that can execute on a variety range of hardware devices, such as cloud servers, mobile devices, and resource-constrained devices.

#### B. Flowchain

Flowchain is the blockchain technology for the IoT developed on Devify. In a blockchain network, the consensus system can ensure the trusted transactions among all IoT nodes in a p2p network. The blockchain for the IoT technology comprises of a p2p network system, and a consensus system. The traditional public blockchains, such as Bitcoin [12] and Ethereum, use proof-of-work (PoW) consensus system; however, the PoW consensus system does not provide the ability of near real-time transactions. Therefore, in our previous work, Flowchain has also already proposed an IoT blockchain technology and a mining based proof-of-stake (PoS) miner to ensure the real-time transactions for IoT blockchain. Consequently, IoT devices vary, e.g., resource-constrained devices, mobile devices, and high-performance server nodes that the computing power varies from devices. Flowchain uses the Devify software framework as the underlying p2p network system to implement such IoT blockchain technology. Thus it can execute on various IoT devices.

### 1.2 Type of Blockchains

The blockchains could be either a public blockchain or a private related to who is allowed to join the blockchain network [7].

#### A. Public Blockchain

Anyone can join the blockchain network, meaning that the blockchain network is entirely open to users for submitting transactions, accessing shared ledgers, and mining. More specifically, since the creation of Bitcoin in 2009, the public blockchain can enable a decentralized model that it can operate without any central authorizations; thus the public blockchain has the nature of openness and trust.

Reviewed Research Paper

**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.*

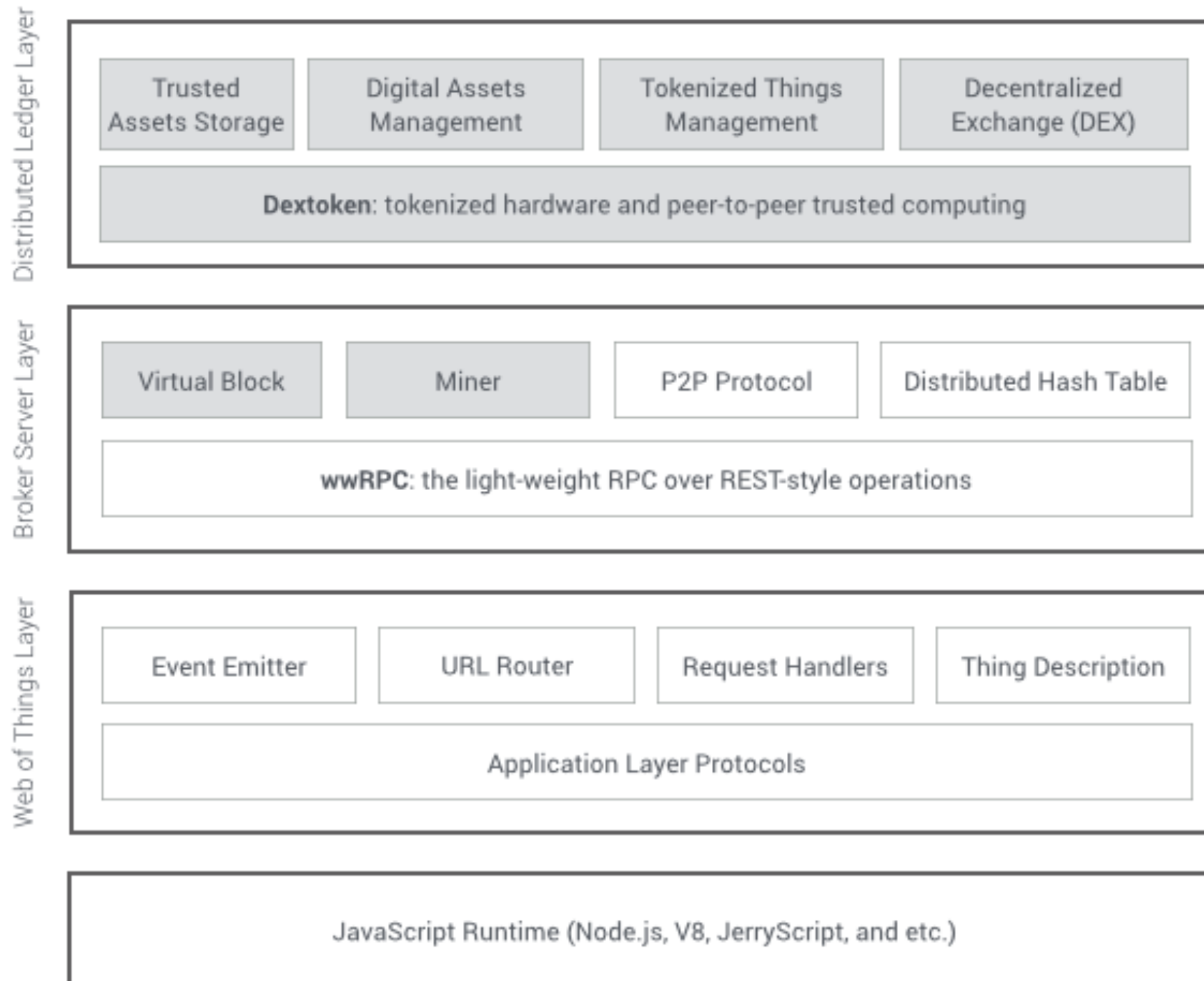
# The Flowchain Insides

- ⦿ The dataflow blockchain
- The Blockchain OS for IoT
- ⦿ The Hybrid blockchain for IoT
- ⦿ Decentralized AI

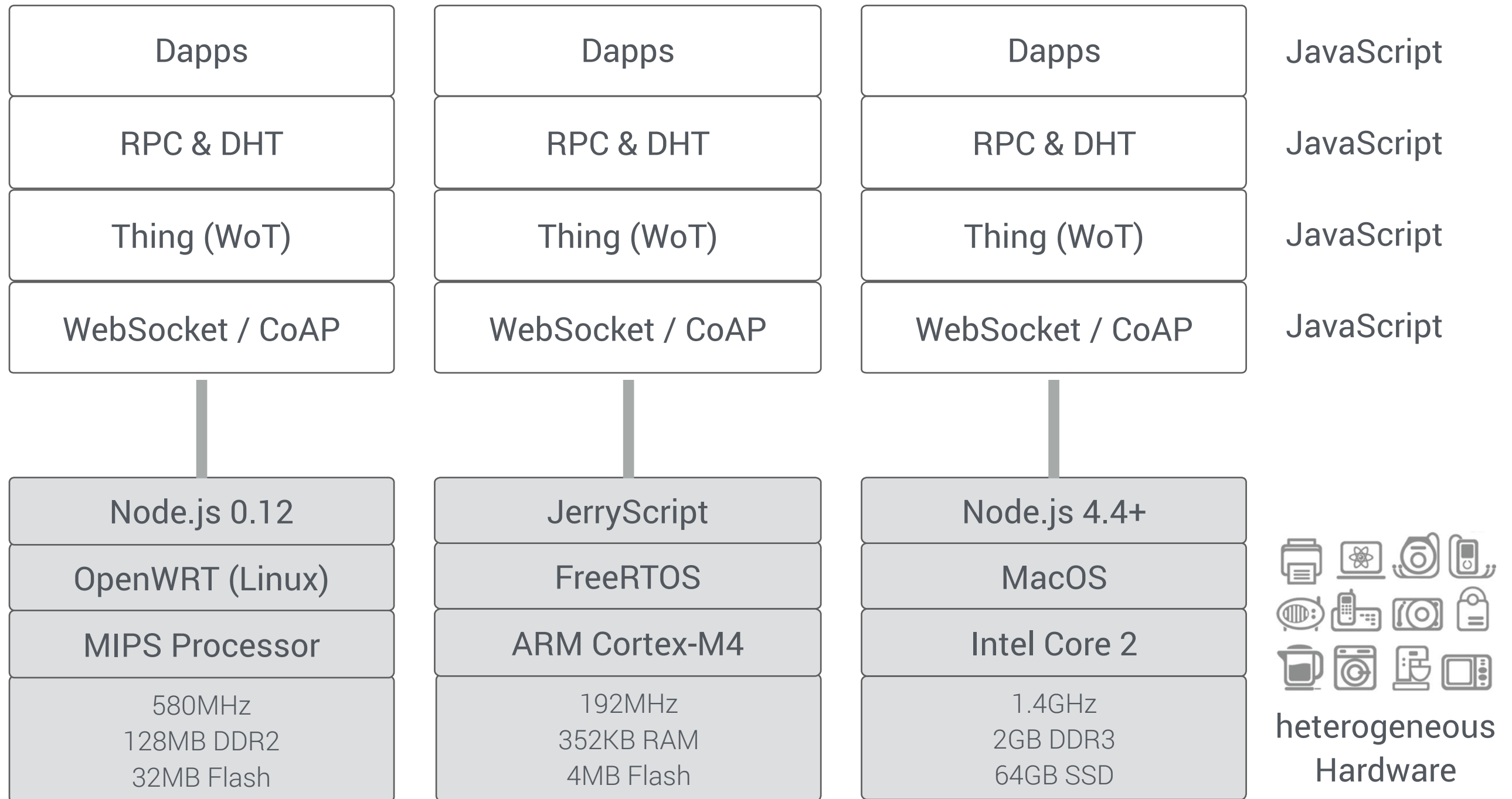
# Blockchain OS, #2 of 4



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

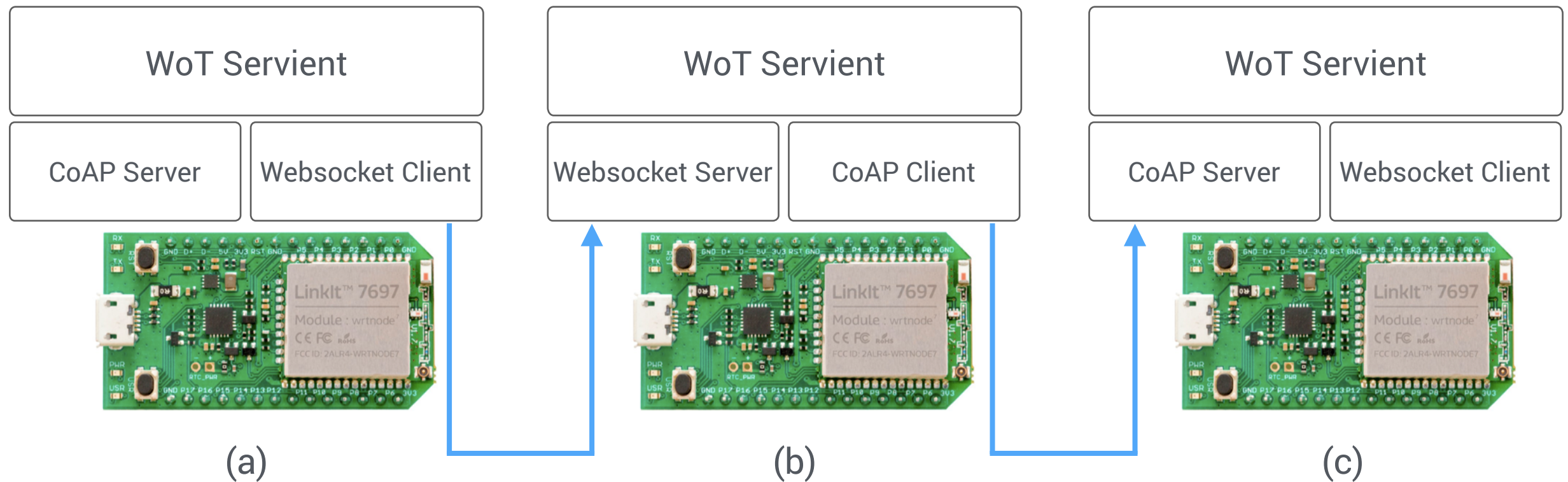


# Flowchain OS runs **Everywhere**



# The Broker Server Layer

- A WoT Servient comprises of client and server combinations.







## SIGBED Review, Volume 15, Number 2, March 2018 Special Issue on Advances in IoT Architecture and Systems (AloTAS'17)

### Content:

- [Where is PELE? Pervasive localization using wearable and handheld devices](#)  
*Luis Henrik John<sup>1</sup>, Chayan Sarkar<sup>2</sup>, and R. Venkatesha Prasad<sup>1</sup>*  
<sup>1</sup>*Delft University of Technology, Delft, The Netherlands*  
<sup>2</sup>*TCS 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 Banerjee<sup>1</sup>, Tanushyam Chattopadhyay<sup>1</sup>, Arpan Pal<sup>1</sup>, and Utpal Garain<sup>2</sup>*  
<sup>1</sup>*TCS Research & Innovation, Kolkata, West Bengal, India*  
<sup>2</sup>*Indian 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 V<sup>1</sup>, Vishwas Shashidhar<sup>2</sup>, G S Aishwarya Meghana<sup>2</sup>, R. Venkatesha Prasad<sup>3</sup>, and Garani Vittal Pranavendra<sup>4</sup>*  
<sup>1</sup>*Indian Institute of Science, Bangalore, India*  
<sup>2</sup>*NITK, Surathkal, Mangalore, India*  
<sup>3</sup>*Delft University of Technology, Delft, The Netherlands*  
<sup>4</sup>*Indian Institute of Technology, Bhubaneswar, India*



### Editorial Board:

- [Sergiy Bogomolov](#), Australian National University, Australia
- [Oleg Sokolsky](#), University of Pennsylvania

# The Flowchain Insides

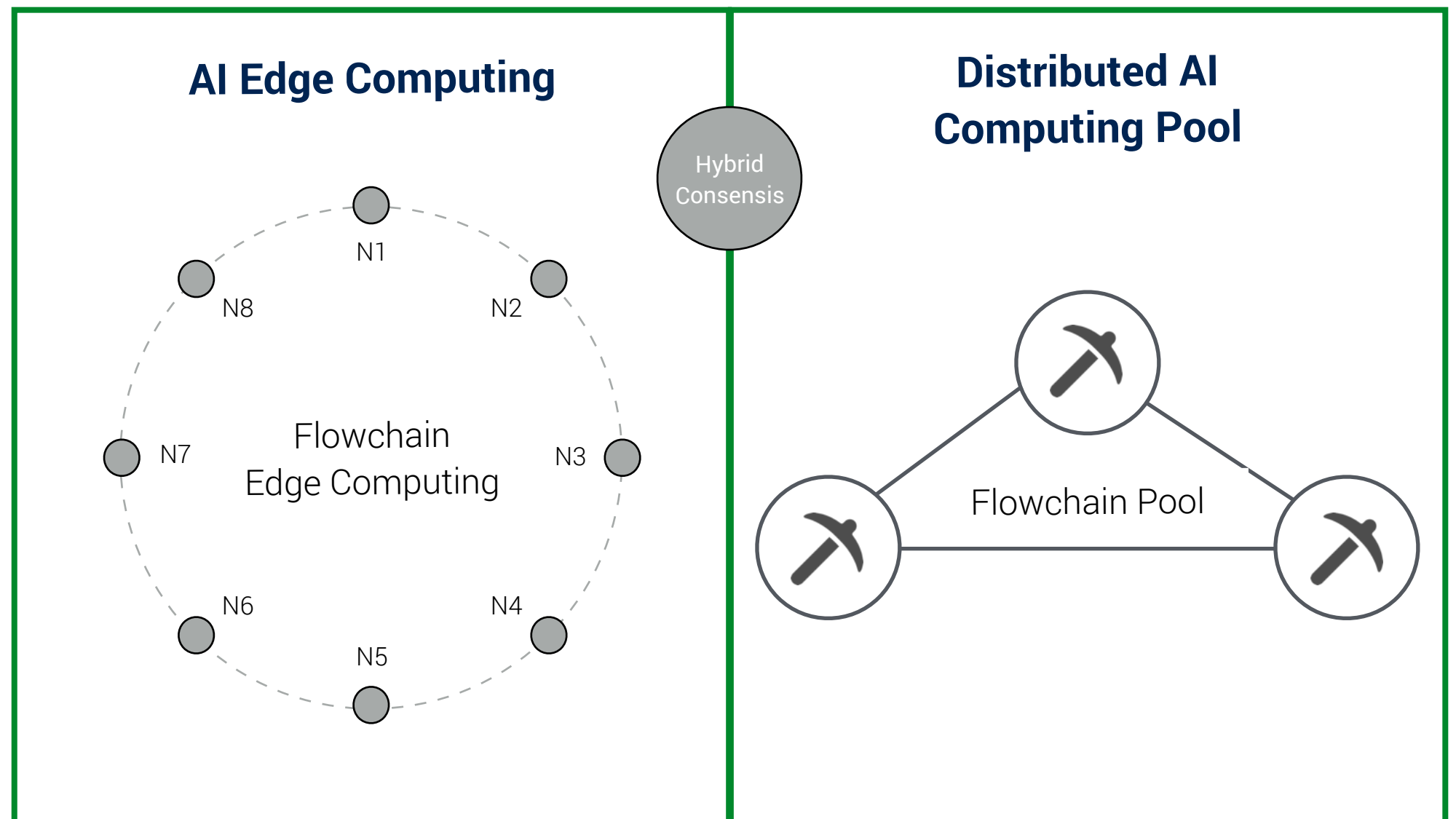
- ⦿ The dataflow blockchain
- ⦿ The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- ⦿ Decentralized AI



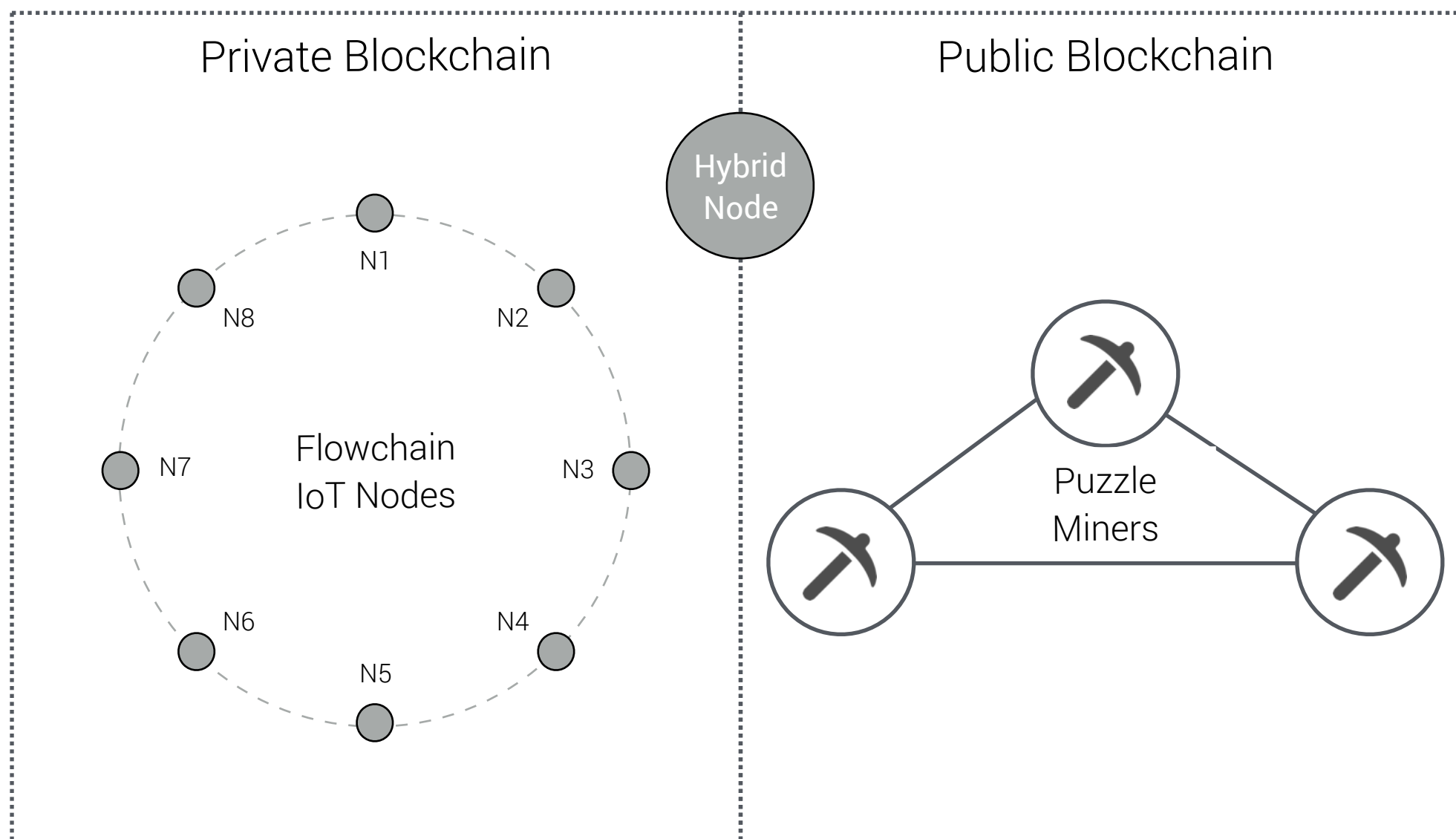
# Hybrid Blockchain, #3 of 4



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



- 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

- ① The dataflow blockchain
- ② The Blockchain OS for IoT
- ③ The Hybrid blockchain for IoT
- ④ Decentralized AI

# Decentralized AI, #4 of 4



Company A  
(Flowchain Edge AI)

Company B  
(Flowchain Edge AI)

Flowchain Hybrid Node

Company C  
(Flowchain Edge AI)

**AI Miners &  
AI Computing Pool**

Flowchain Hybrid Node

Flowchain Hybrid Node

Company F  
(Flowchain Edge AI)

Flowchain Hybrid Node

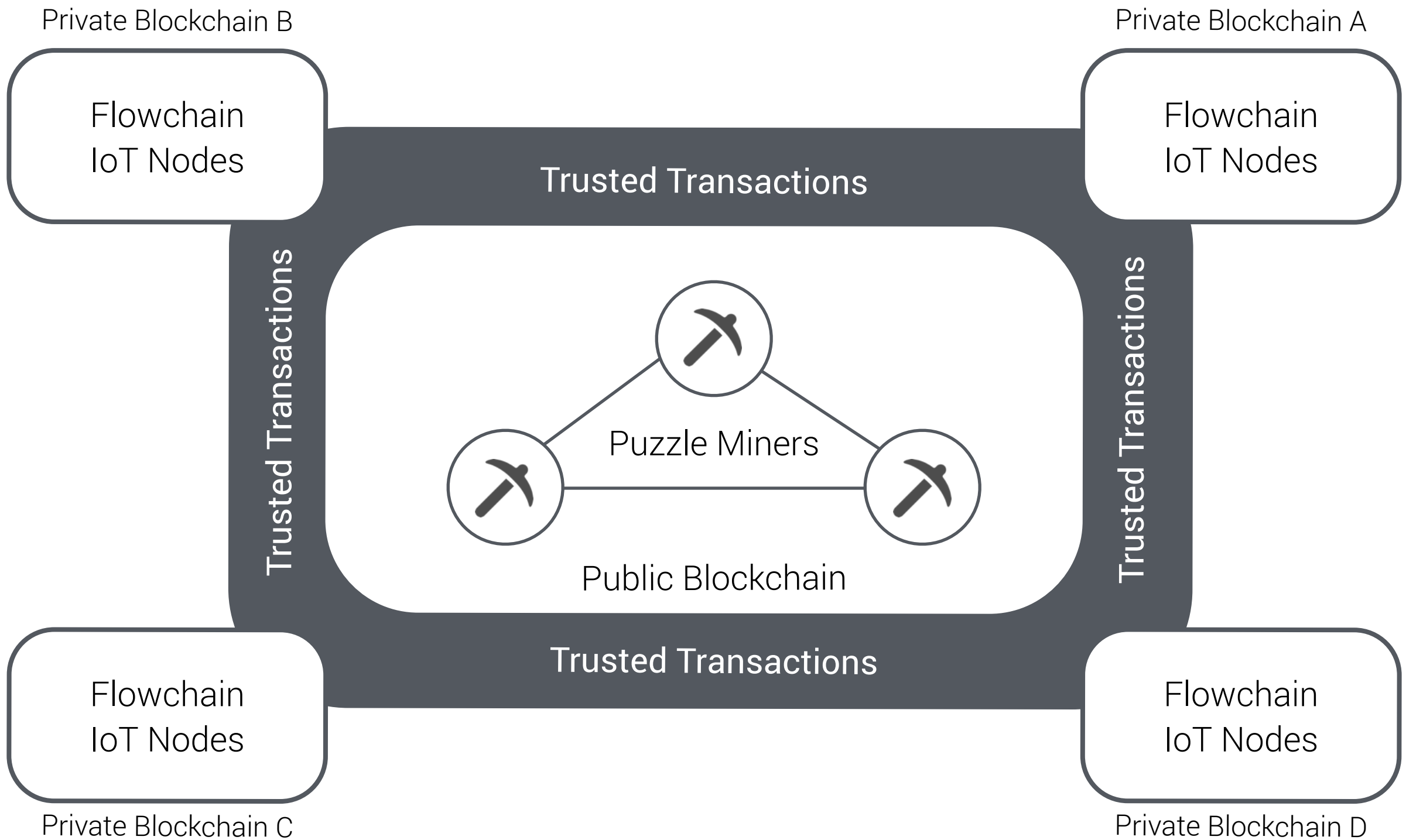
Company D  
(Flowchain Edge AI)

Company E  
(Flowchain Edge AI)

# **Flowchain**

## Pseudonymous Authentication

# IoT Blockchain + AI over **Pseudonymous Authentication**



# Academic Papers



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

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

### ABSTRACT

This paper addresses the issue of current Internet of Things (IoT) development - the decentralized IoT model - as a mixture of a peer-to-peer network and interoperable IoT devices. This paper proposes a new IoT software architecture, the Devify software framework, to address the peer-to-peer IoT network and the interoperable IoT device development. Besides, the work also shows through experiments that an IoT application server can simply use the flow-based programming (FBP) paradigm to define the application as a data exchange network. Therefore, the software architecture also provides each FBP runtime environment for writing IoT applications.

### Keywords

Internet of Things, Interoperability, Peer-to-Peer, Web of Things, Decentralized, Flow-Based Programming

### 1. INTRODUCTION

In recent years, the development of Internet of Things (IoT) applications has become increasingly complex. This complexity has motivated us to address the problem by providing the ability to connect IoT data to the IoT platform over the web to simplify the creation of IoT applications [1]. However, current existing IoT platforms are the centralized model that they act as brokers or hubs to connect the exchanged data between IoT devices. Therefore, most studies expect that IoT should use the decentralized model to ensure secure data exchange and data privacy. Thus, this paper proposes a decentralized IoT software framework to provide the ability of secure data exchange between IoT devices automatically without any centralized server. In short, the purpose of a new design for the IoT software architecture is that we need a *devify* programming framework to support each full range hardware devices. Besides, the Devify software framework implements the requirements of emerging IoT trends: (1) the peer-to-peer networking for IoT devices, (2) a full stack devify software framework, (3) the device interoperability via REST-style HTTP operations, and (4) the use of the Web of Things (WoT) and JSON-LD ontology.

The rest of this paper is structured as follows: we describe the motivation of this work in Section 2, and subsequently



Figure 1: The Devify Architectural Design

study the related work in Section 3. In Section 4, we introduce the proposed software framework and review what technologies are adopted in the software framework. In Section 5, we review the design and implementation details of the peer-to-peer network as well as the way to address the problem of data in peer-to-peer network. In Section 6, we propose the use of the flow-based programming (FBP) paradigm to create the IoT application server. In Section 7, we show two Devify application examples. We conclude in Section 8.

### 2. MOTIVATION

The motivation of this paper is to develop a generic and comprehensive software framework for building various types of new IoT networks in a decentralized manner. Also, current IoT network comprises a variety range of hardware devices, such as cloud servers, mobile devices, and resource-constrained devices (like heterogeneous IoT hardware devices). Thus, the software framework must be able to monitor on all these hardware devices. Since the blockchain has become a significant technology in the proximity of IoT hardware devices, this paper proposes a REST-like devify programming framework for the software framework to support each IoT hardware.

Furthermore, the motivation of the decentralized IoT should address the device interoperability and a peer-to-peer network, thus, this paper will also address such technical challenges. In this work, we attempt to build a generic software framework for future development of decentralized IoT applications. Among the potential decentralized IoT applications, the nature of the distributed ledger technology (DLT) has a huge opportunity to build a new peer-to-peer IoT network. Therefore, we have already developed Flowchain [2], the blockchain for the IoT, to practically prove the concept of this work.

Copyright retained by the authors.

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.*

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

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

**Abstract.** Recently, the blockchain for the IoT has combined an emerging technology for creating secure access and data real-time IoT systems. Despite a great of studies on blockchain IoT, few studies have investigated how an IoT blockchain system works in practice. In this paper, we propose Flowchain, an open source distributed ledger programming framework for peer-to-peer IoT networks and real-time data transactions. The main feature of the Flowchain framework is Virtual Blocks that provides the new blockchain data structure design to ensure the real-time data transaction. This paper also propose a software architecture that provide peer-to-peer IoT networking and interoperable IoT application framework.

**Keywords.** Blockchain, Distributed Ledger, IoT, P2P, WoT, JSON-LD

### 1. Introduction

Blockchain, a frequently referenced environment, uses a distributed database system called a blockchain [3]. The Bitcoin blockchain can operate without any central server that the transactions stand with high trust. Although the Bitcoin blockchain has such decentralized network model, it does not meet the need of current IoT requirements. As the Bitcoin blockchain uses "mined proof" to create new transactions, the average waiting time for verifying a transaction could be 10 minutes that not in a real-time manner. Thus, to address this technical challenge, the main aim of the Flowchain programming framework is to provide a *devify* blockchain system for the IoT that can process and record transactions in a real-time manner. Flowchain presents a new architecture called Virtual Blocks to provide each real-time transaction ability.

Besides, Bitcoin uses a distributed single blockchain model in which all nodes compete to mine new blocks. However, IoT hardware nodes, e.g., resource-constrained devices, mobile devices, and high-performance server nodes that the computing power varies from devices. Thus, resource-based functions have been proposed to deal with heterogeneous hardware [4]. The mining process

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.*

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

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

### ABSTRACT

This paper addresses the issue of *secure and trusted* Internet of Things (IoT) networks by adopting the emerging blockchain technologies. This paper proposes a new hybrid blockchain technology to address the trusted IoT issues such as trustless communications and decentralized applications. Besides, we also present that the pseudonymous authentication technique can use a puzzle-solving computation to enable trustless communications for the IoT and provide the capabilities of near real-time transactions. In our previous work, we presented a decentralized software framework for the IoT by using a p2p network and the concept of the blockchain. In this paper, we outline the core components of the hybrid blockchain and delve deeper the algorithms of the *Hybrid consensus* to provide the capabilities for our hybrid blockchain technology.

### Keywords

Internet of Things, Blockchain, Hybrid Consensus, Peer-to-Peer, Trustless Computing, Decentralized

### 1. INTRODUCTION

The Internet of Things (IoT) devices can generate and exchange security-critical data over the IoT network. Many IoT networks use the public-key infrastructure (PKI) to authenticate devices and ensure the data security as well as the data privacy. The IoT device has to sign the generated data by a digital public key, and deliver the data to the network for exchanging. However, such authentication method tends to be expensive for an IoT device regarding computing power and energy consumption.

Furthermore, the blockchain technology has the decentralized, secure, and private nature to become a promising idea that can be approaching the next-generation IoT architecture. Therefore, in our previous work, Flowchain and Devify have already been proposed to build a blockchain technology for the IoT device over a p2p network. Therefore, to achieve a secure and *inexpensive* blockchain for the IoT, this paper proposes *Flowchain Hybrid Blockchain* to enable *fast authentication* by eliminating the concept of traditional PKI methods. Furthermore, our work can address the technical challenge of achieving an efficient and secure IoT device to exchange the captured data by the blockchain technology.

Copyright retained by the authors.

The rest of the paper is organized as follows: In Section 2 we describe the main components of the hybrid blockchain design. In Section 3 we present the model including the architecture, algorithms and the hybrid blockchain design. The IoT blockchain economy is discussed in Section 4. Finally, Section 5 concludes the paper.

### 1.1 Previous Works

#### A. Devify

Devify has already proposed a generic and comprehensive software framework for building various types of trust IoT networks in a decentralized manner that can execute on a variety range of hardware devices, such as cloud servers, mobile devices, and resource-constrained devices.

#### B. Flowchain

Flowchain is the blockchain technology for the IoT developed on Devify. In a blockchain network, the consensus system can ensure the trusted transactions among all IoT nodes in a p2p network. The blockchain for the IoT technology comprises of a p2p network system, and a consensus system. The traditional public blockchains, such as Bitcoin [12] and Ethereum, use proof-of-work (PoW) consensus system; however, the PoW consensus system does not provide the ability of near real-time transactions. Therefore, in our previous work, Flowchain has also already proposed an IoT blockchain technology and a mining based proof-of-stake (PoS) miner to ensure the real-time transactions for IoT blockchain. Consequently, IoT devices vary, e.g., resource-constrained devices, mobile devices, and high-performance server frames that the computing power varies from devices. Flowchain uses the Devify software framework as the underlying p2p network system to implement such IoT blockchain technology. Thus it can execute on various IoT devices.

### 1.2 Type of Blockchains

The blockchain could be either a public blockchain or a private related to who is allowed to join the blockchain network [7].

#### A. Public Blockchain

Anyone can join the blockchain network, meaning that the blockchain network is entirely open to users for submitting transactions, accessing shared ledgers, and mining. More specifically, since the creation of Bitcoin in 2009, 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.

Reviewed Research Paper

**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.*

# 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**.

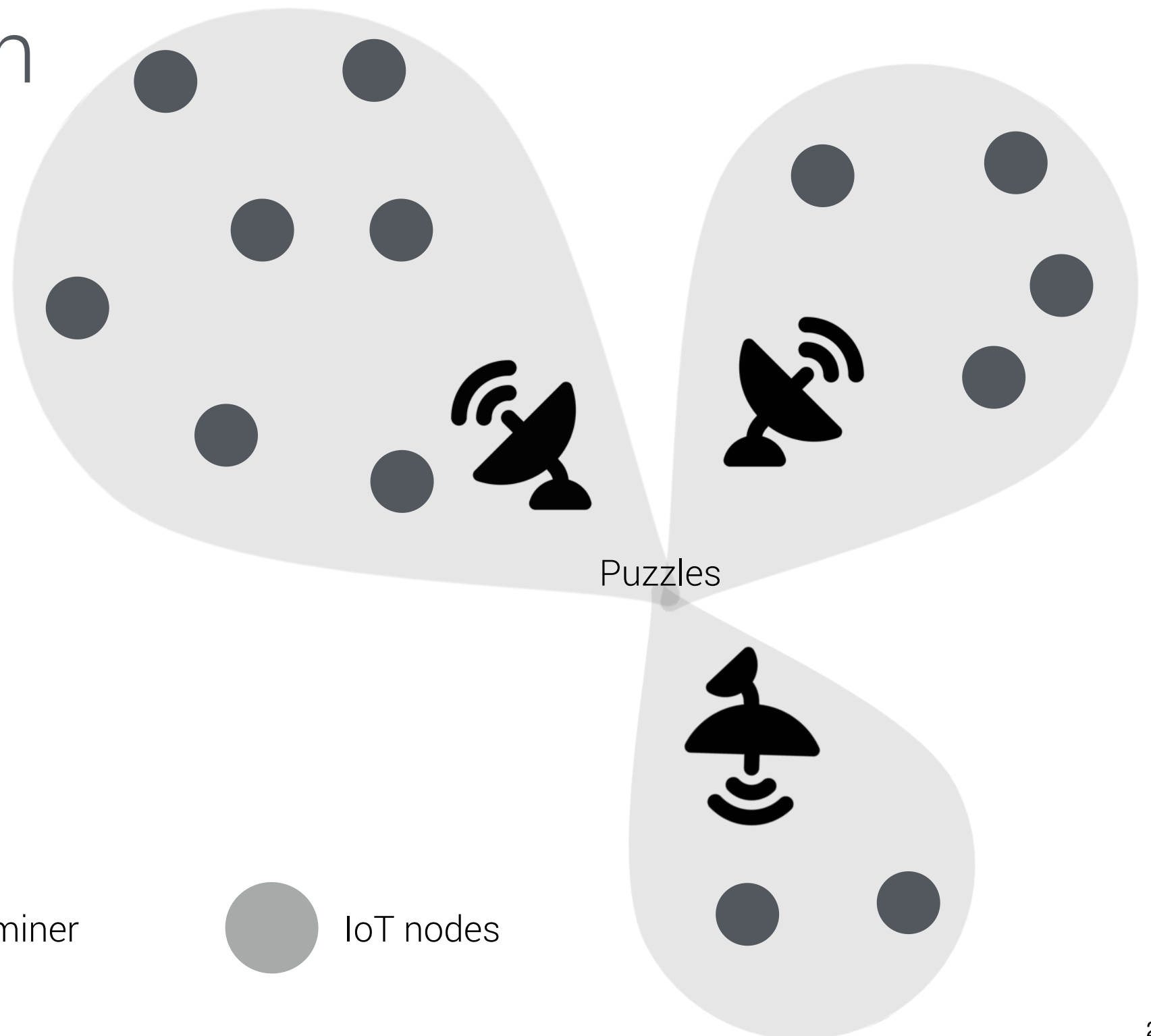


# Private Blockchains

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.

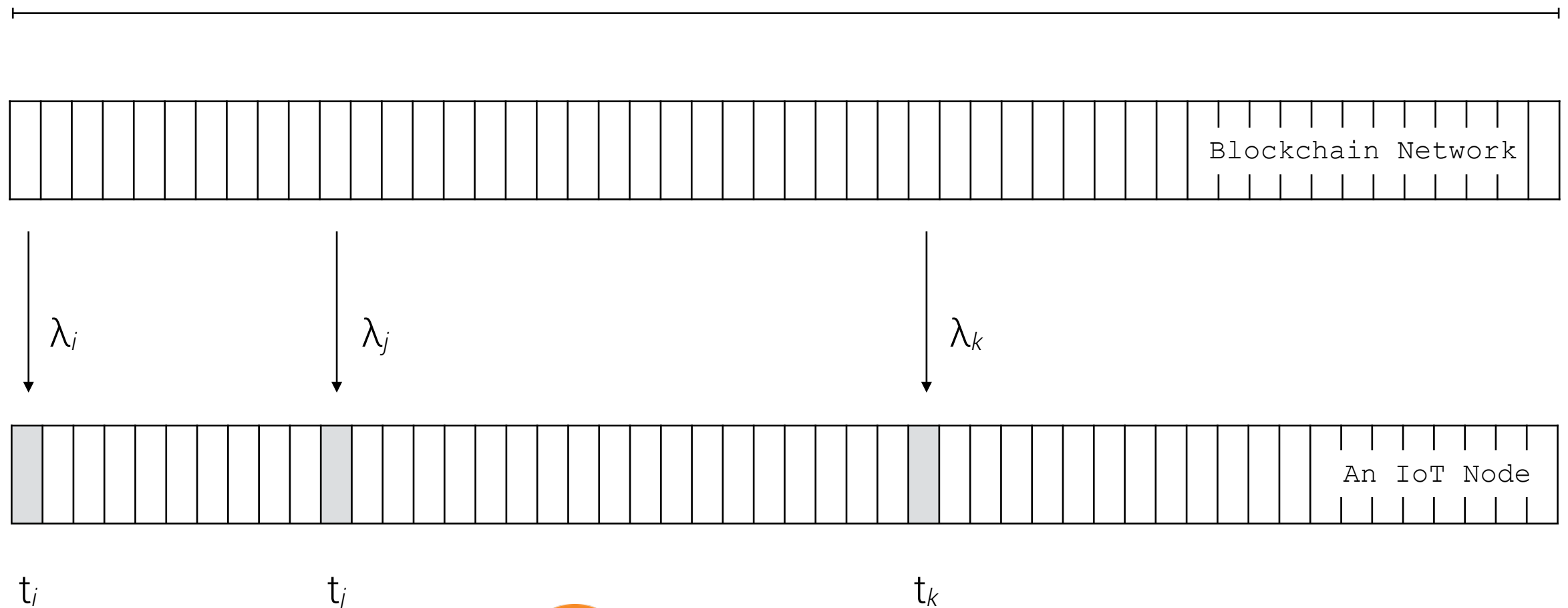
# Pseudonymous authentication can replace the PKI to enable a fast authentication



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

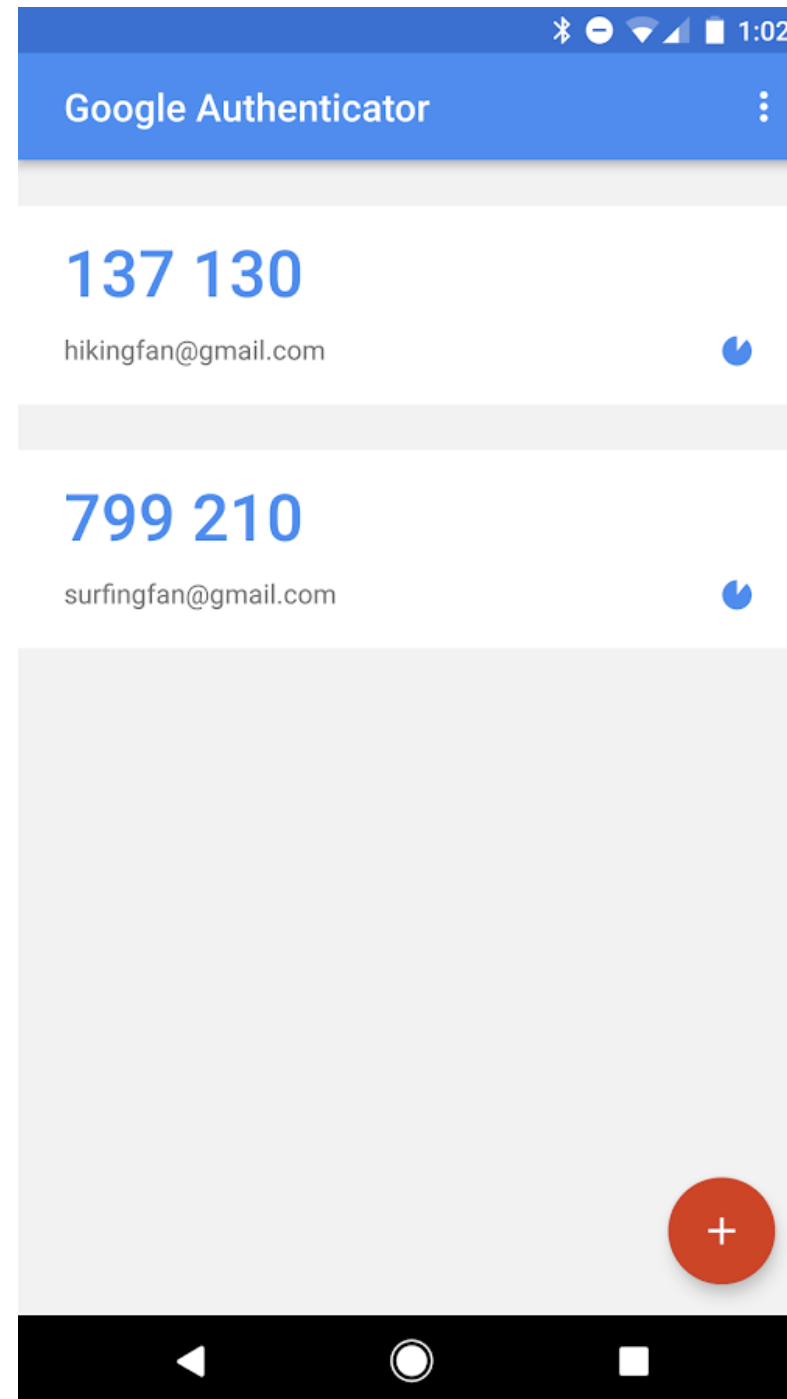
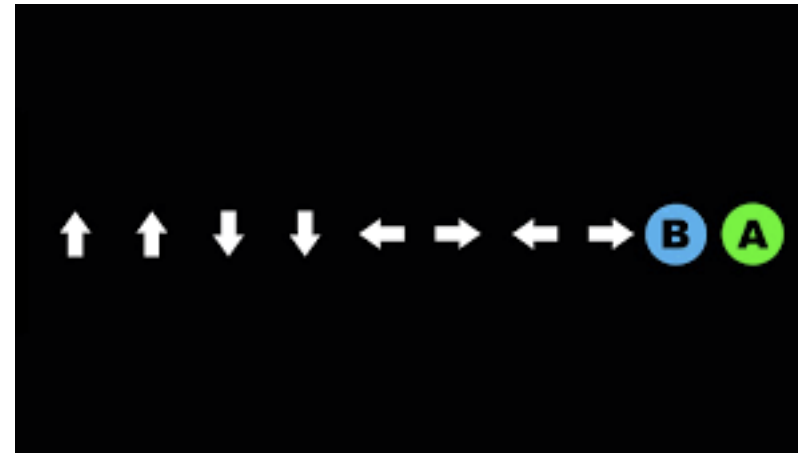
The IoT node was pseudonymously authenticated to submit transactions at  $(t_i, t_j, t_k)$ .

Fix period scheduling: 1 second = 50.0 slices (50 kHz)



λ

a truly random  
Konami Code  
that only  
validate in a  
fixed time  
period





```
/**
```

```
* The lambda value has to be unique, truly random, and unattackable. So that, ideally, the value  
* has to be a nonce value that can solve the shared work which has a lower difficulty., Currently,  
* in the PoC stage, we just set the shared difficulty at a fixed value.
```

```
*/
```

```
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



**Hybrid Flowchain: Smart Contract Platform for Distributed Autonomous Machines**

1.  $U_i$  starts receiving  $\lambda$  from the broadcasting
2. Let  $Puzzle$  be a function and  $\xi_j$  be a string;  $U_i$  receives a puzzle  $(Puzzle, x_j)$  from a peer  $U_j$  in the private blockchain over the p2p network
3. Let  $Puzzle(\lambda)$  gives an arbitrary-length vector  $\vec{x}$  of the Konami Code, then  $\vec{x} = (x_1, \dots, x_n), n < j$
4. Let  $\mathcal{F}_{puz}$  maintain a set  $\mathcal{T}$  of puzzle solutions, then  $\mathcal{F}_{puz}$  computes each entries in  $\vec{x}$ , let  $y_i = \mathcal{F}_{puz}(x_i), i = (1, \dots, j)$
5. The miners say that  $U_i$  solves the puzzle  $(Puzzle, x_j)$  if  $\mathcal{F}_{puz}$  successfully finds  $y_i = x_j$  within the time interval  $\sigma$
6.  $\mathcal{F}_{puz}$  returns  $\xi_j$  to  $U_j$  and stores  $\mathcal{H} = (\vec{x}, y_i, \lambda)$  in  $\mathcal{T}$
7. The miners and  $U_j$  confirm the user  $U_i$  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  $(sk_i, pk_i)$ ; 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

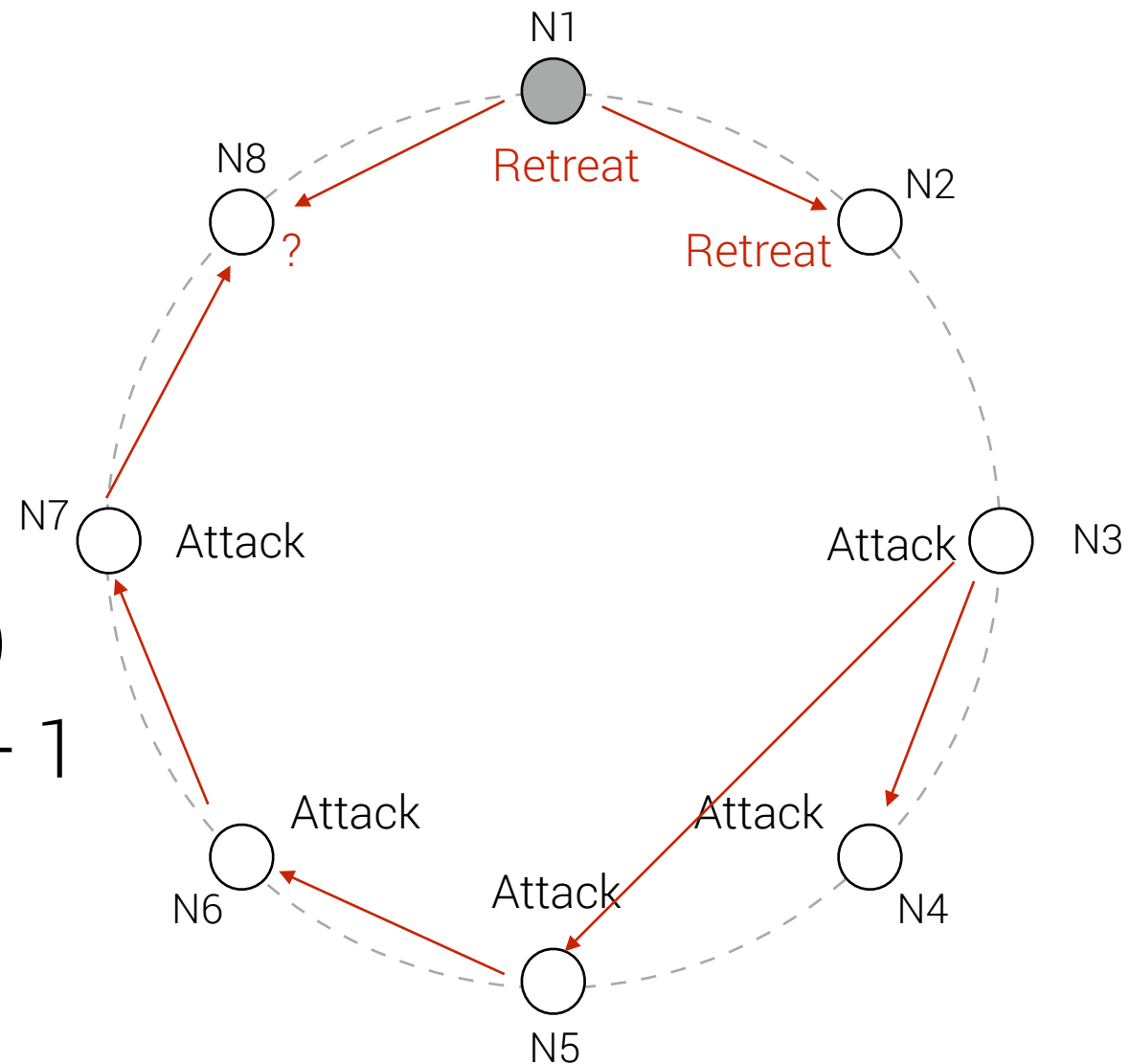
# Byzantine Fault Tolerance

➔  $n = 8$

➔  $\pi = 1$

➔  $n > 3\pi + 1$

➔ for  $n$  in  $[N1..N8)$   
 $f_{\text{conn}}(n) > 2\pi + 1$



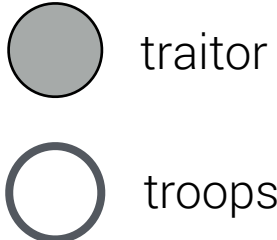
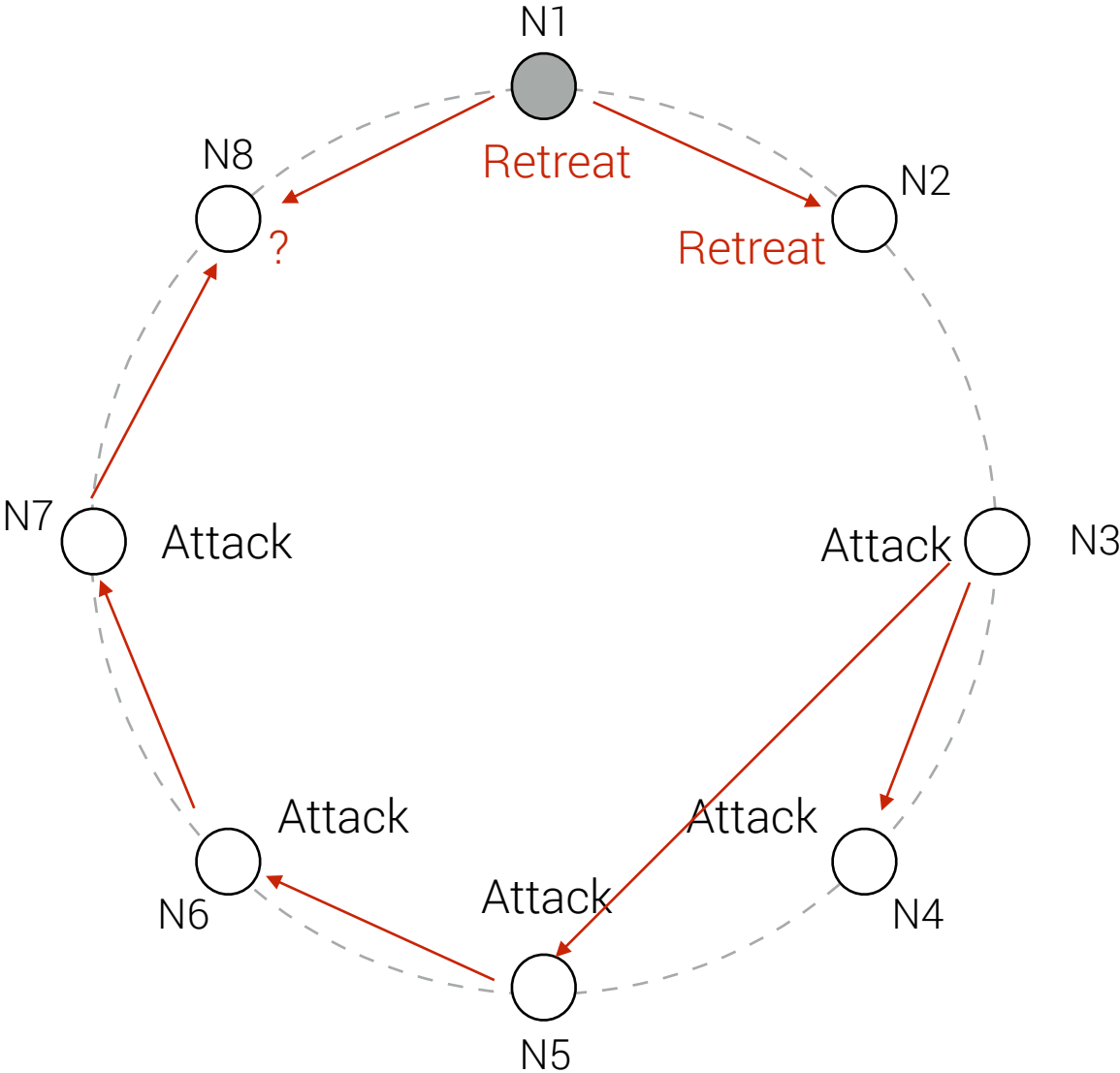
● traitor

○ troops

# Flowchain BFT



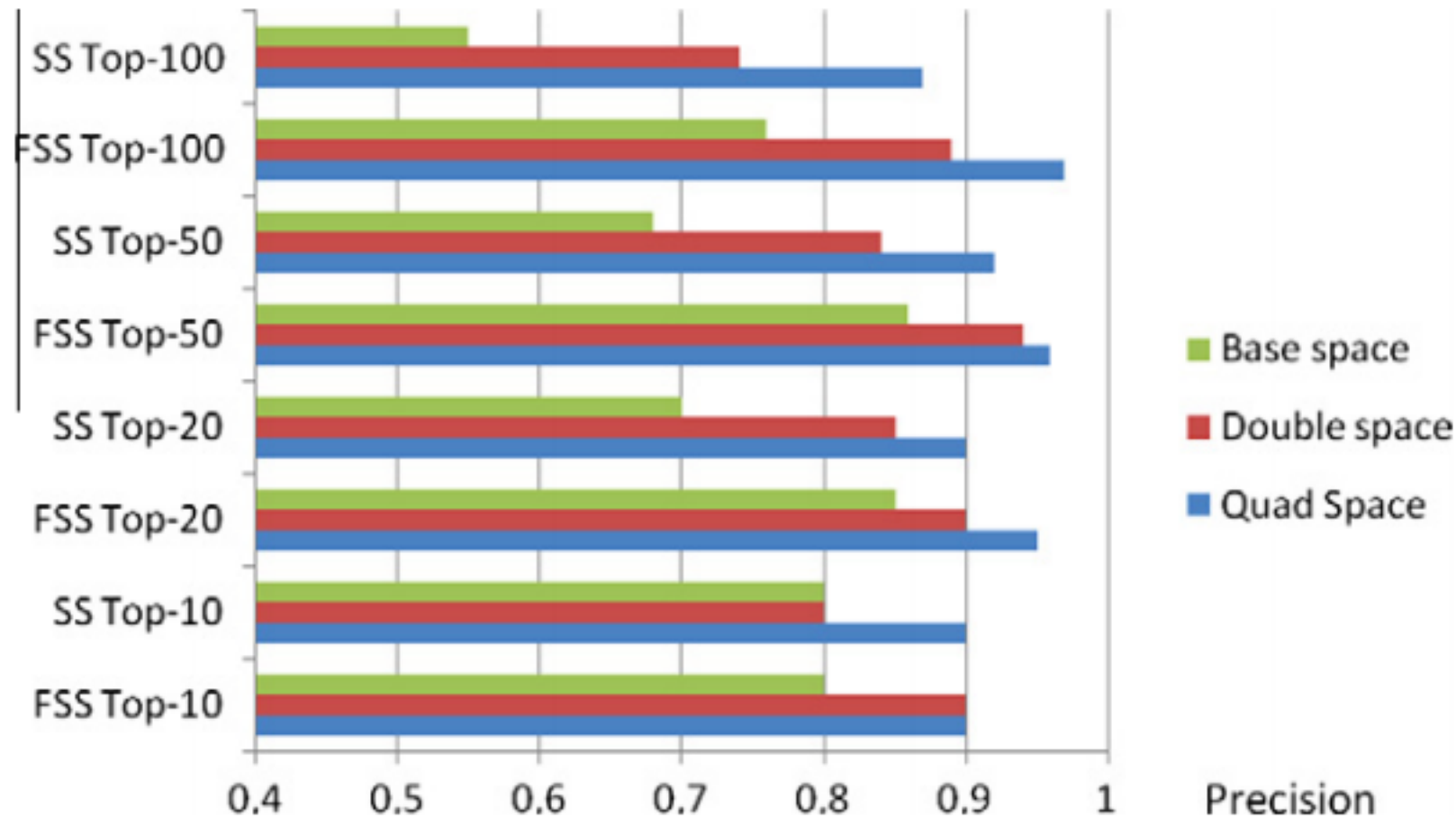
- ➔  $n = 8$
- ➔  $\pi = 1$
- ➔  $n \geq \pi + 1$
- ➔ Faulty PEs free



# 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

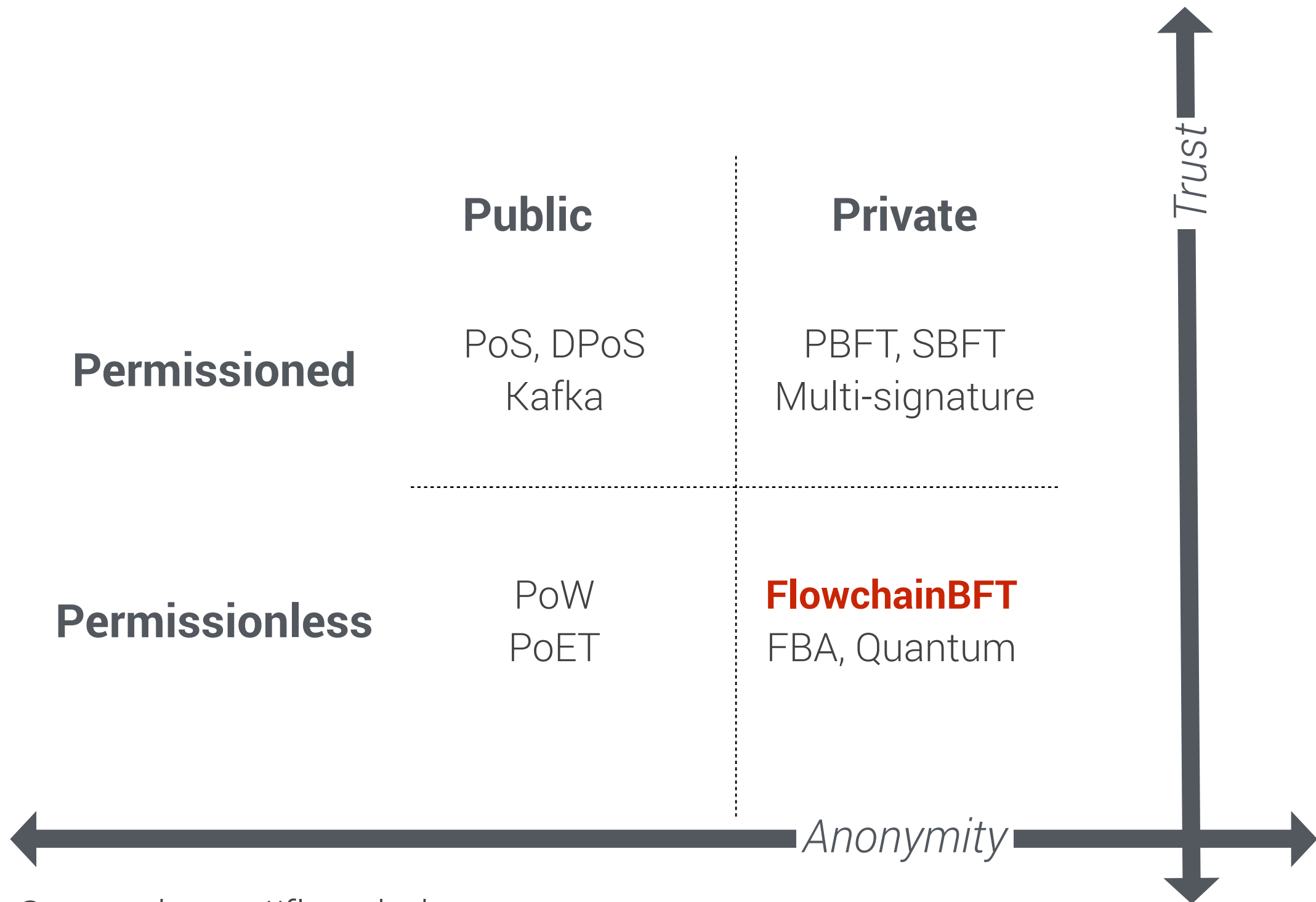


**Fig. 10.** Top- $k$  Precision with increasing space in Trials 5.

# 基於 BFT 的共識算法

	Dolev	Fekete	FCA	CCA	Flowchain BFT	Brooks- lyengar
<b>Maximum faulty PEs</b>	$N/3$	$N/4$	$N/3$	$N/3$	$N/2$	$N/3$
<b>Complexity</b>	$N\pi$	N/A	$O(N)$	N/A	$O(N)$	$O(N)$
<b>Order of network bandwidth</b>	$O(N)$	$O(N)$	$O(N)$	$O(N)$	$O(N)$	$O(N)$
<b>Convergence rate</b>	$1/(N-2\pi-1)$	$1/((N-2\pi)/\pi)$	$2\pi/N$	$\pi/N$	2*accuracy	$2\pi/N$

# Trust and Anonymity



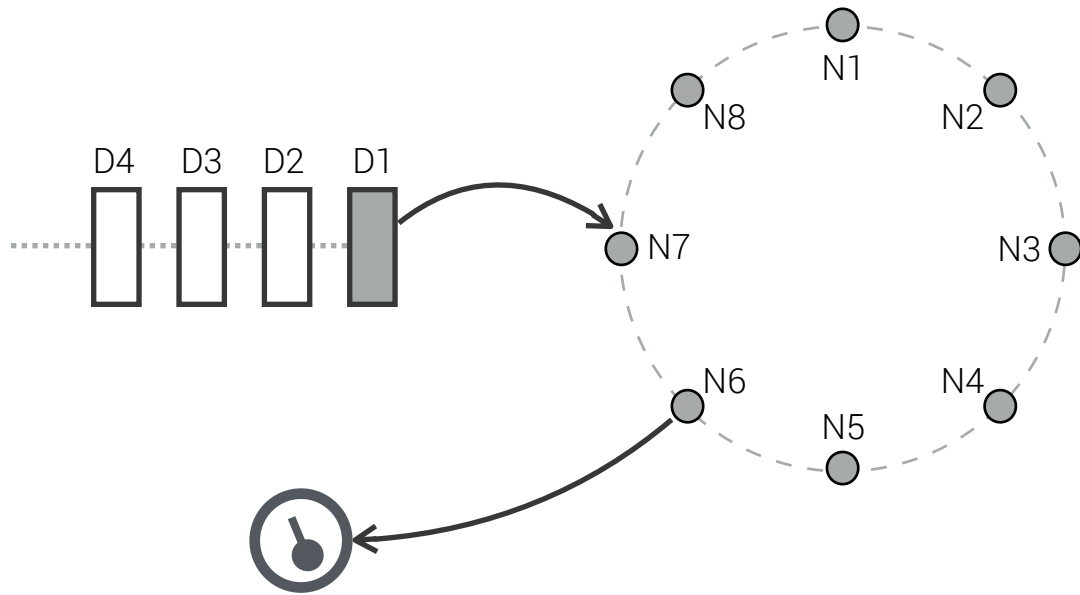
Source: <https://flowchain.co>

**Flowchain**

Submit

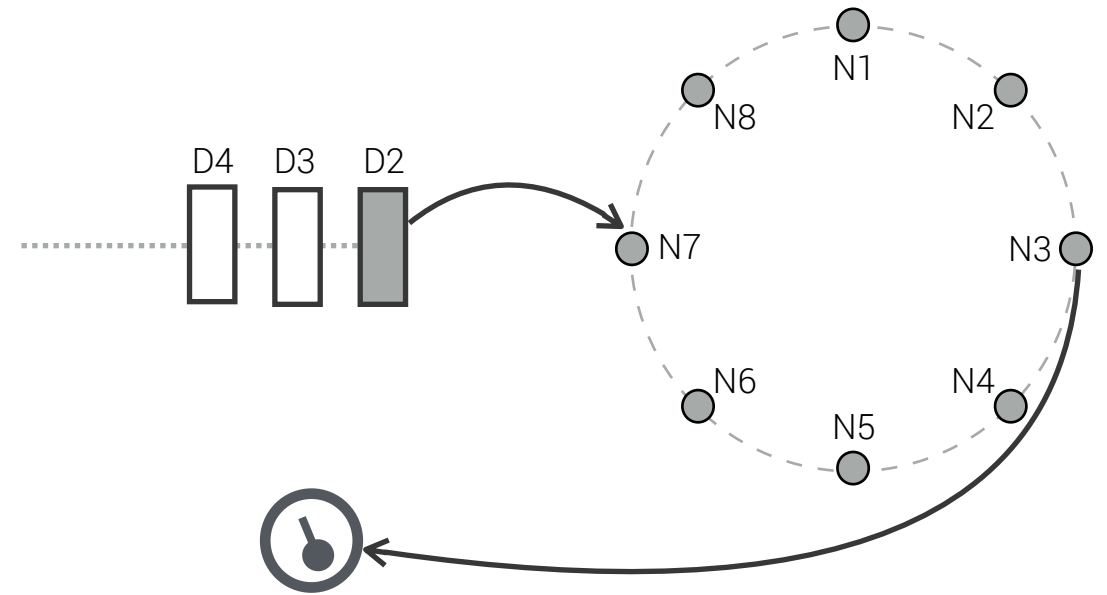
Transactions

SUCCESSOR(D1) = N6



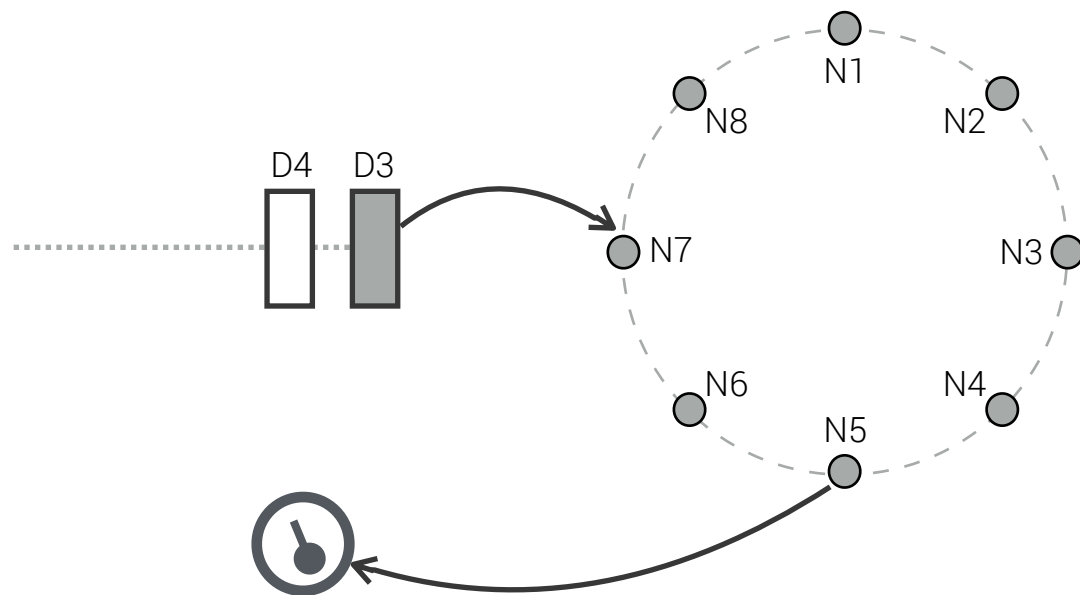
(a)

SUCCESSOR(D2) = N3



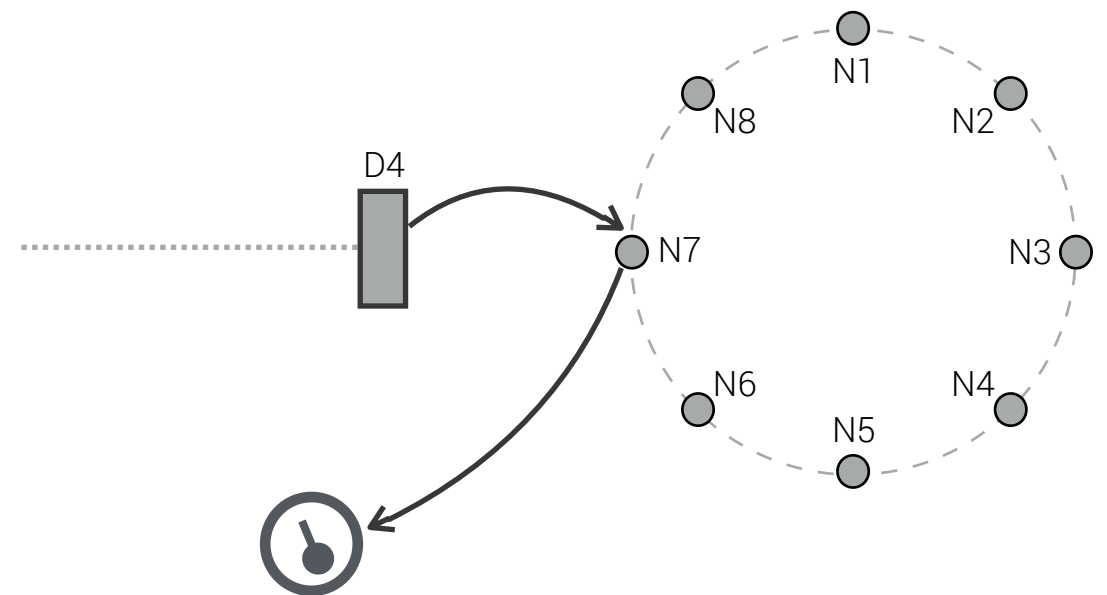
(b)

SUCCESSOR(D3) = N5

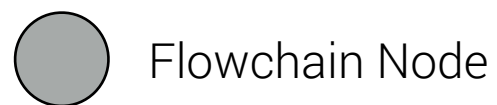


(c)

SUCCESSOR(D4) = N7

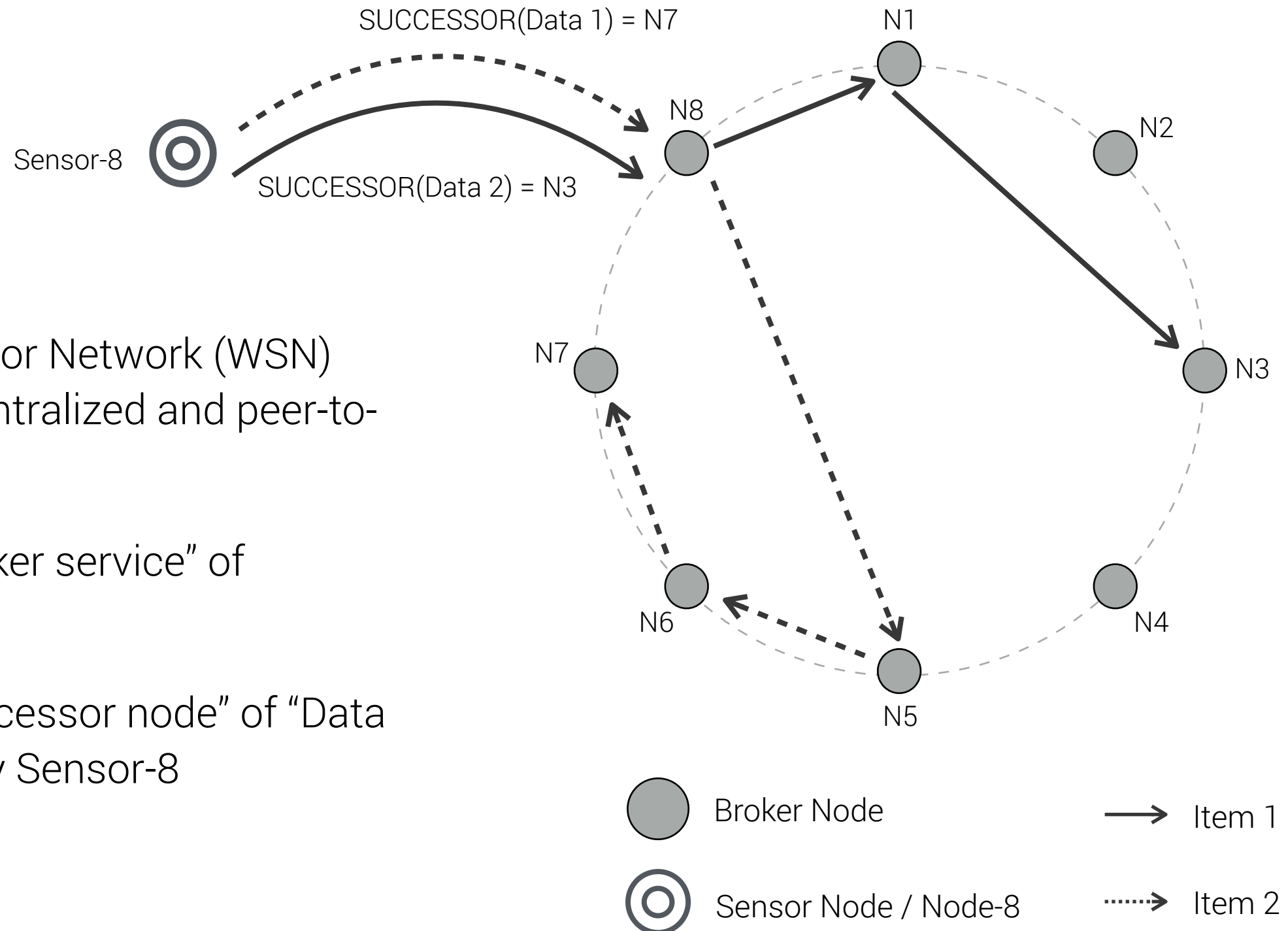


(d)





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

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

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

Lookup the successor node in the DHT

# Generating Transaction ID



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

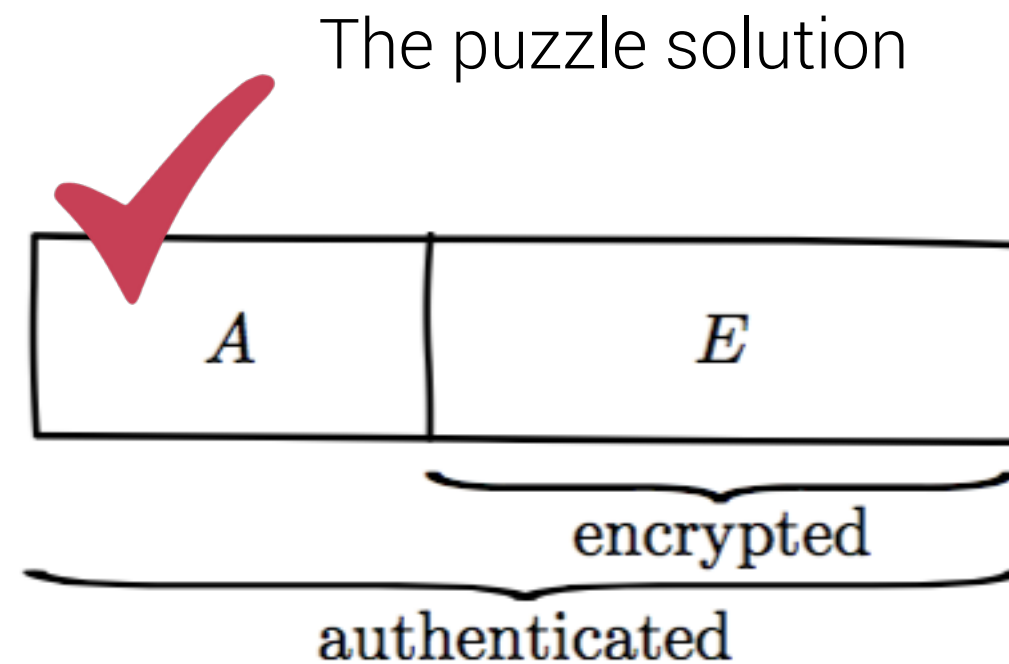
$$\mathbf{H}_{\text{BLOCK}} = \mathbf{SHA256}(\text{BlockNo} + \text{timestamp} + \text{nonce})$$

$$\mathbf{H}_{\text{DATA}} = \mathbf{SHA1}(\text{data} + \text{timestamp} + \lambda)$$

$$\mathbf{H}_{\text{txID}} = \mathbf{SHA256}(\mathbf{SHA256}(\mathbf{H}_{\text{BLOCK}} + \mathbf{H}_{\text{DATA}}))$$

- **The data transaction process (E)**
  - Step 1: Generate the key of the data -  $\mathbf{H}_{DATA}$
  - Step 2: Search the successor node of the key in the DHT -  $\text{SUCCESSOR}(\mathbf{H}_{DATA})$
  - Step 3: Send  $[\mathbf{H}_{DATA}, \lambda]$  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**  $\mathbf{H}_{txID}$  to the public blockchain

# Authenticated Encryption with Associated Data (AEAD)



**Flowchain**

Tokenized

Hardware

# Cooperate on Tokenized Hardware

## Tokenized Hardware: The New Crypto Innovation

Jollen Chen<sup>1</sup> and Eric Pan<sup>2</sup>

<sup>1</sup> Flowchain Open Source Project, Devify Inc.

[jollen@flowchain.io](mailto:jollen@flowchain.io)

<sup>2</sup> Seeed Technology Co.,Ltd.

[ep@seeed.cc](mailto: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.

# 硬件代币化



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.

## 封面故事 Coverstory 專家開講



陳俊宏

仕橙研策科技股份有限公司執行長

Day、Campus 等形式舉辦，例如德國 Chaos Communication Camp 就是知名的駭客大聚會，大部分參加的人純粹是為了好玩，享受許多編程高手齊聚一堂相互切磋交流的樂趣。其次是一些官方或半官方，像是經濟部、資策會這些單位所主導，這一類據我的觀察效果較不如預期，因為獲獎的意圖太者以大專院校 credit，有利手反而興趣缺缺。第三種則是由企業來舉

稱駭客) 協同合作，值得追求創新的企業一起深入思考。

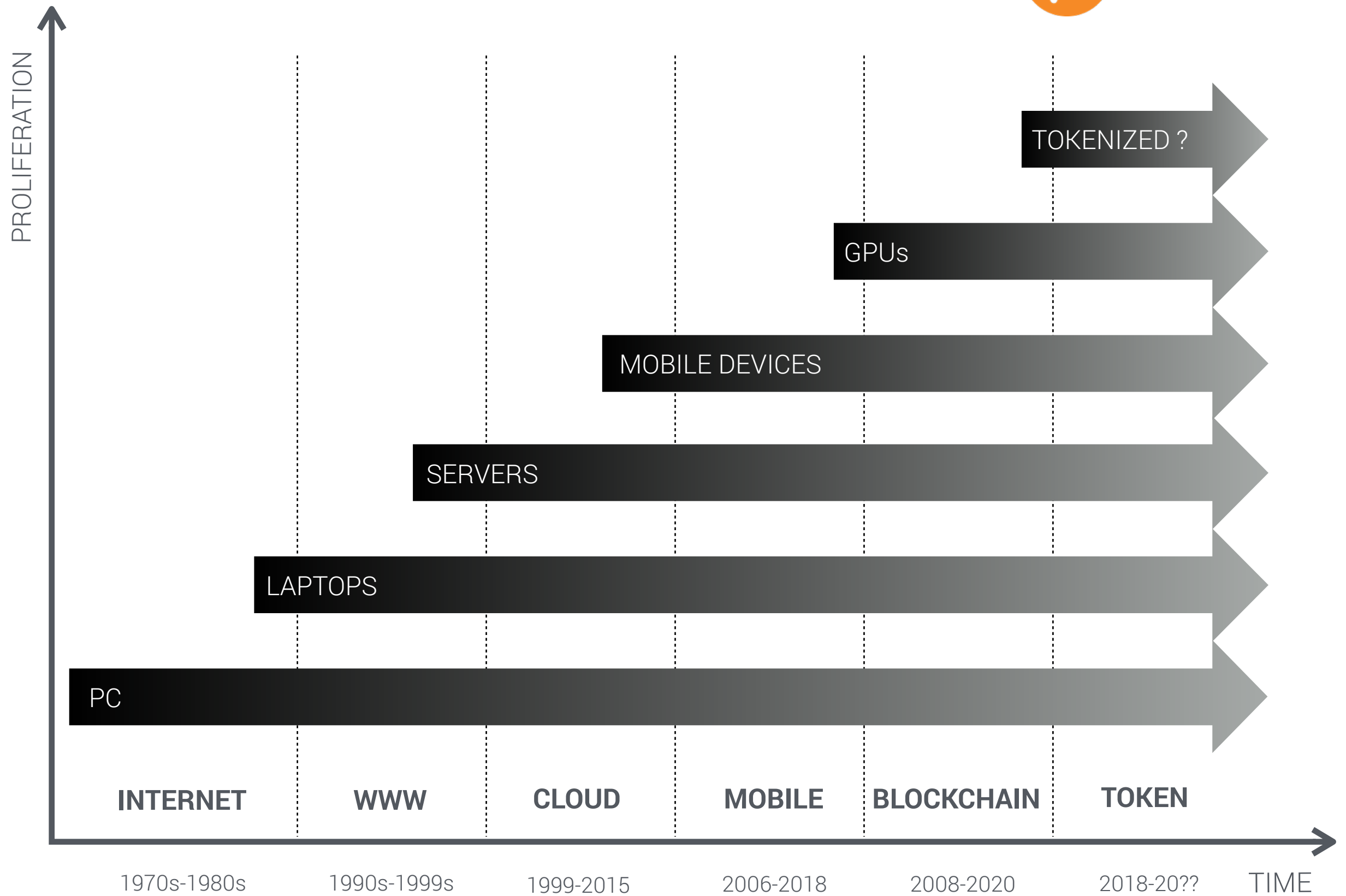
### 洞見勝於技術

企業要如何透過黑客松這一類型的活動尋求創新？回答此一問題前，必須先了解因黑客松而聚集的這群人所擁有的能力

Coverstory Interview by China Productivity Center, 2016

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.





# From Hardware to Tokenized Hardware

Hardware	v.s.	Tokenized Hardware
<ul style="list-style-type: none"><li>• Tangible assets</li></ul>		<ul style="list-style-type: none"><li>• Tangible assets</li><li>• Digital assets</li><li>• Ownership</li><li>• Rights</li><li>• Depreciation</li><li>• Externality</li><li>• Decentralized assets</li></ul> Exchange (Dextoken)

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



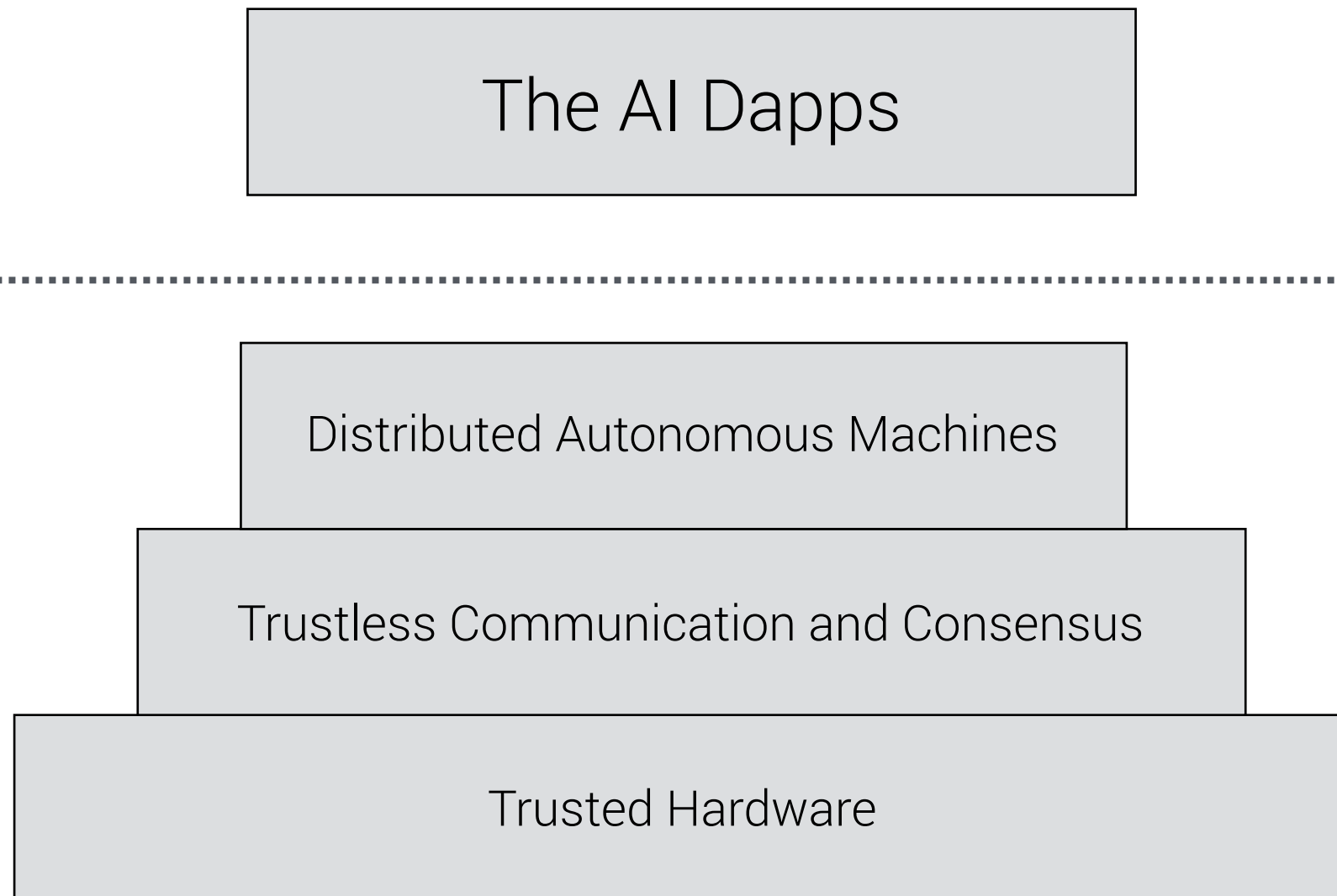
# Conclusions

# 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

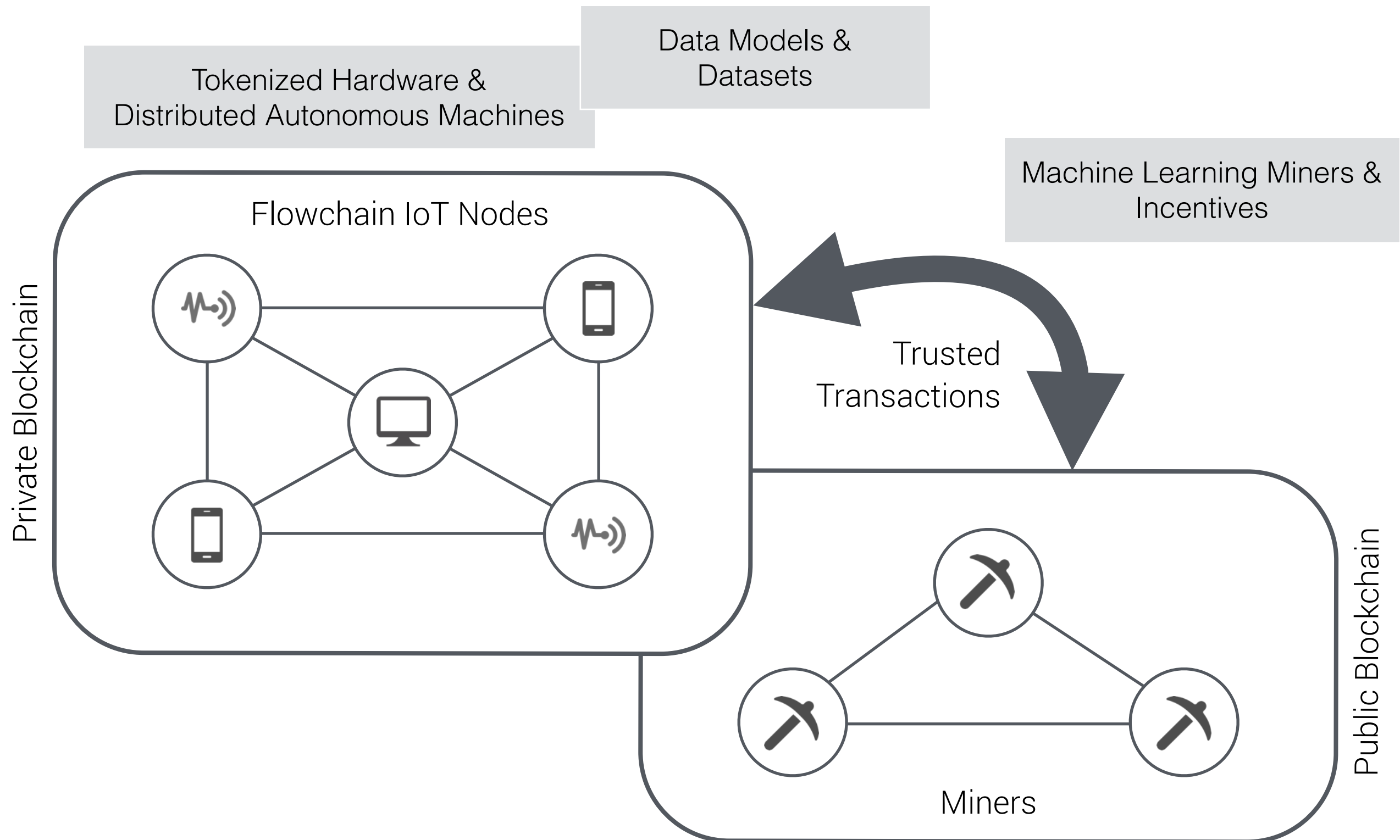


# Flowchain underlying layer: Tokenized Hardware + DAM



	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	
Trusted Third Party (TTP)	HMAC	

# Flowchain uppermost layer: AI over IoT Blockchain



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



FLOWCHAIN

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

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

Contact **[jollen@flowchain.io](mailto:jollen@flowchain.io)**

WeChat **jollentw**