LINUXCON containercon CLOUDOPEN

CHINA 中国

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

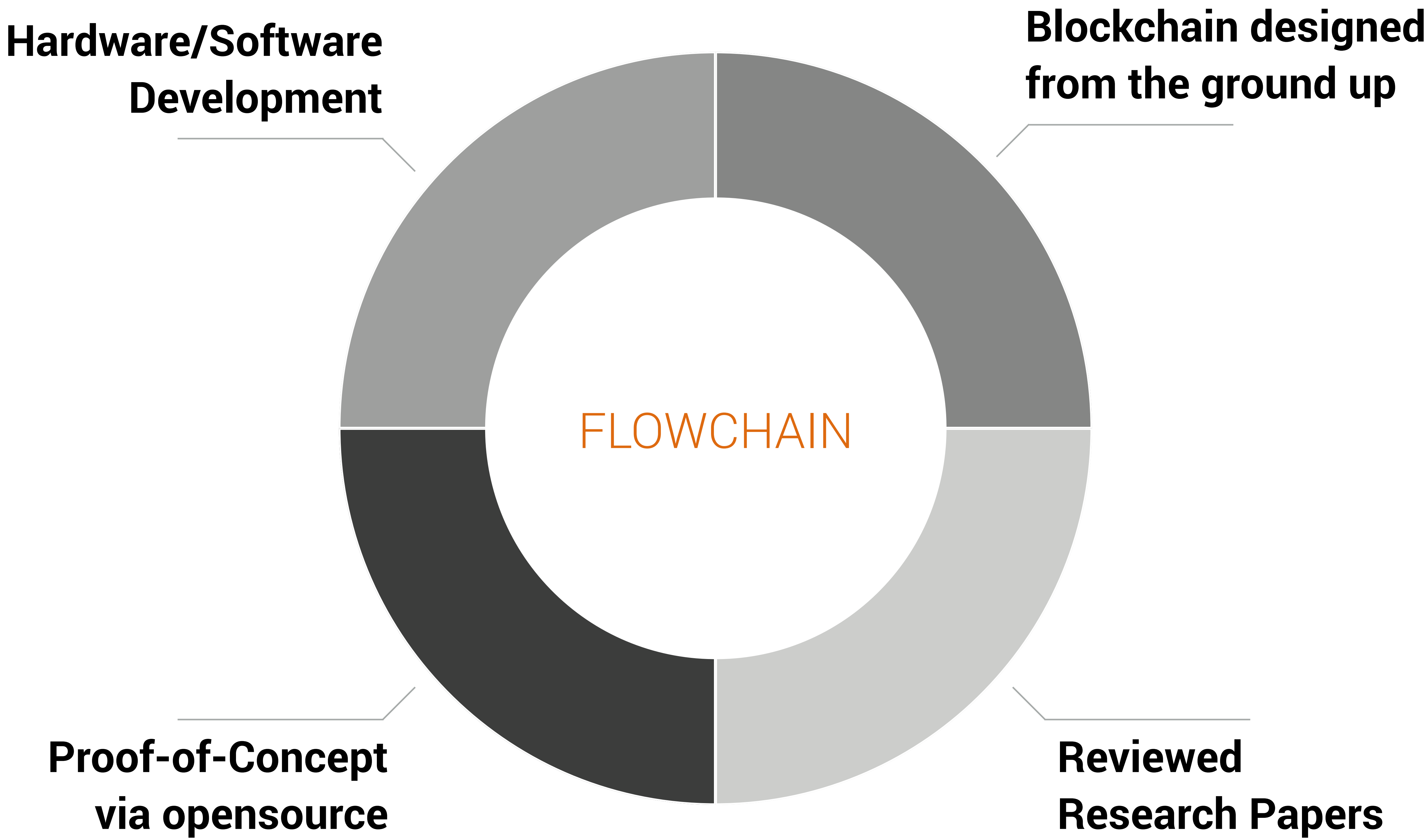
Flowchain = (mining) * (IoT, Blockchain, AI)

mining → Cryptocurrency (Incentives)

IoT, Blockchain, AI → Flowchain Technologies

The Distinguished Aspects

FLOWCHAIN



Free and Open

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

FLOWCHAIN

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 Forks 17

flowchain-app
A Flowchain plugin that provides the flow-based programming (FBP) engine.
JavaScript ★ 26 Forks 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 Forks 18

flowchain-ledger
A distributed ledger for the p2p and decentralized IoT devices in JavaScript.
JavaScript ★ 16 Forks 8

wwRPC
A light weight library that makes REST-style RPC operations over the Websocket
JavaScript ★ 3 Forks 2

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

The Flowchain Insides

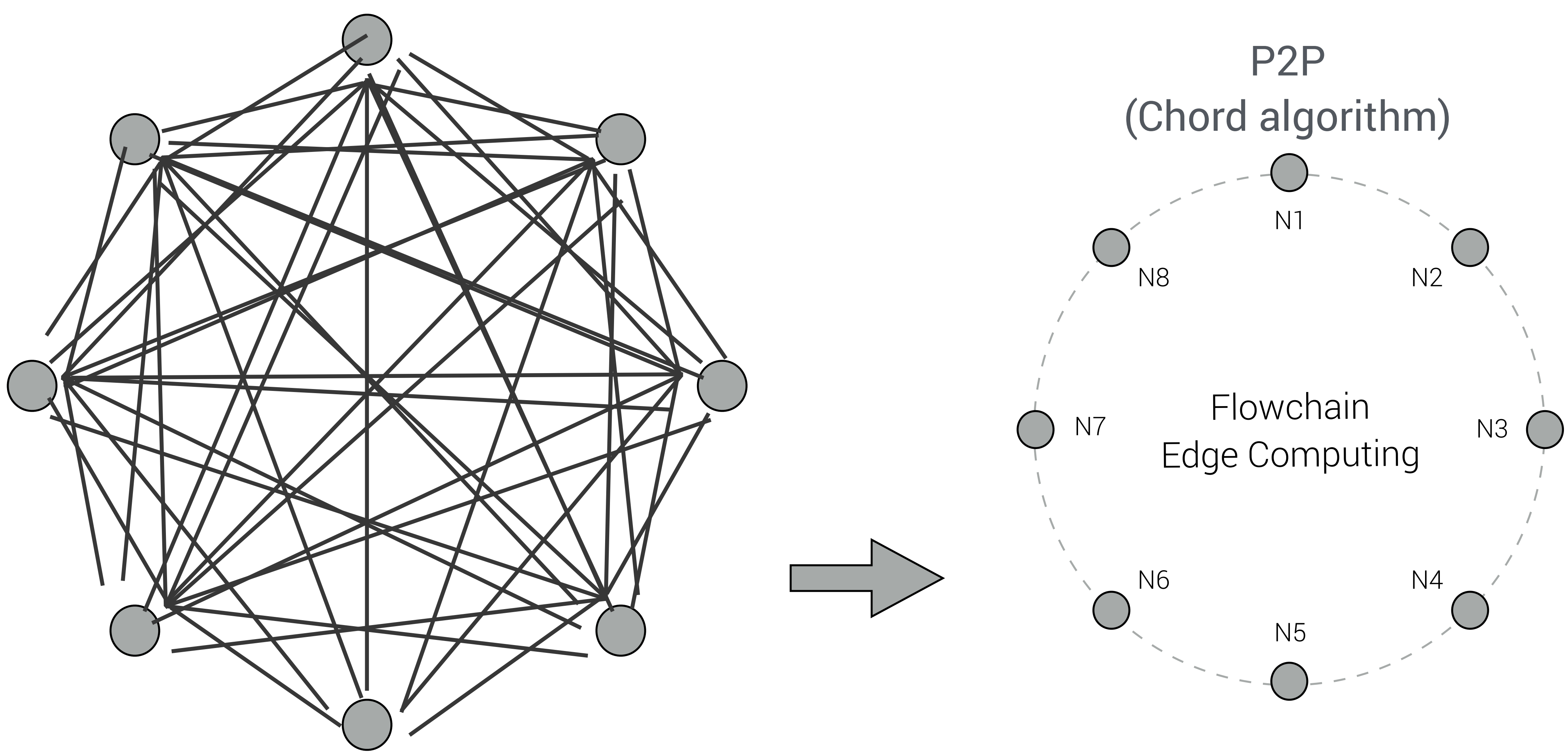
- The data**flow** block**chain**
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI

FLOWCHAIN

Dataflow Blockchain, #1 of 4

FLOWCHAIN

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



Academic Papers

FLOWCHAIN


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

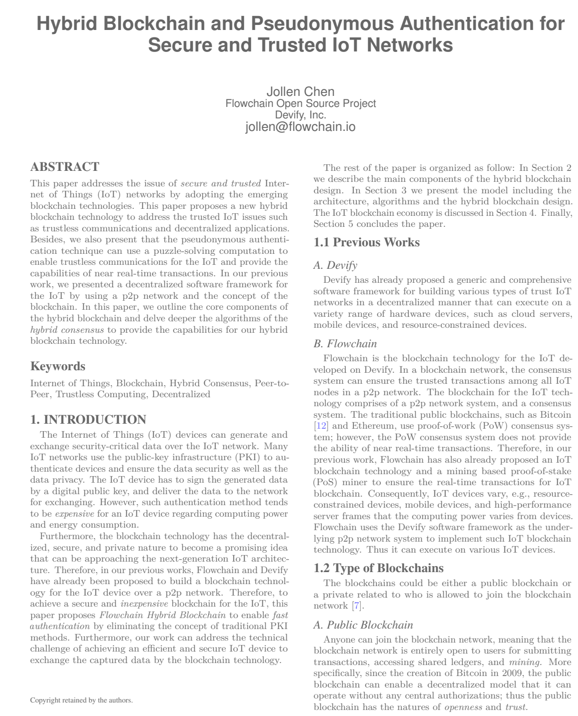
Jollen Chen
Devify Open Source Project
Devify, Inc.
jollen@flowchain.io

Reviewed Research Paper


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

Jollen Chen

Reviewed Research Paper


Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks

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

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.

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

InProceedings of the Workshop on 2nd Advances in IoT Architecture and Systems, June 3, 2018, Los Angeles, USA.

The Flowchain Insides

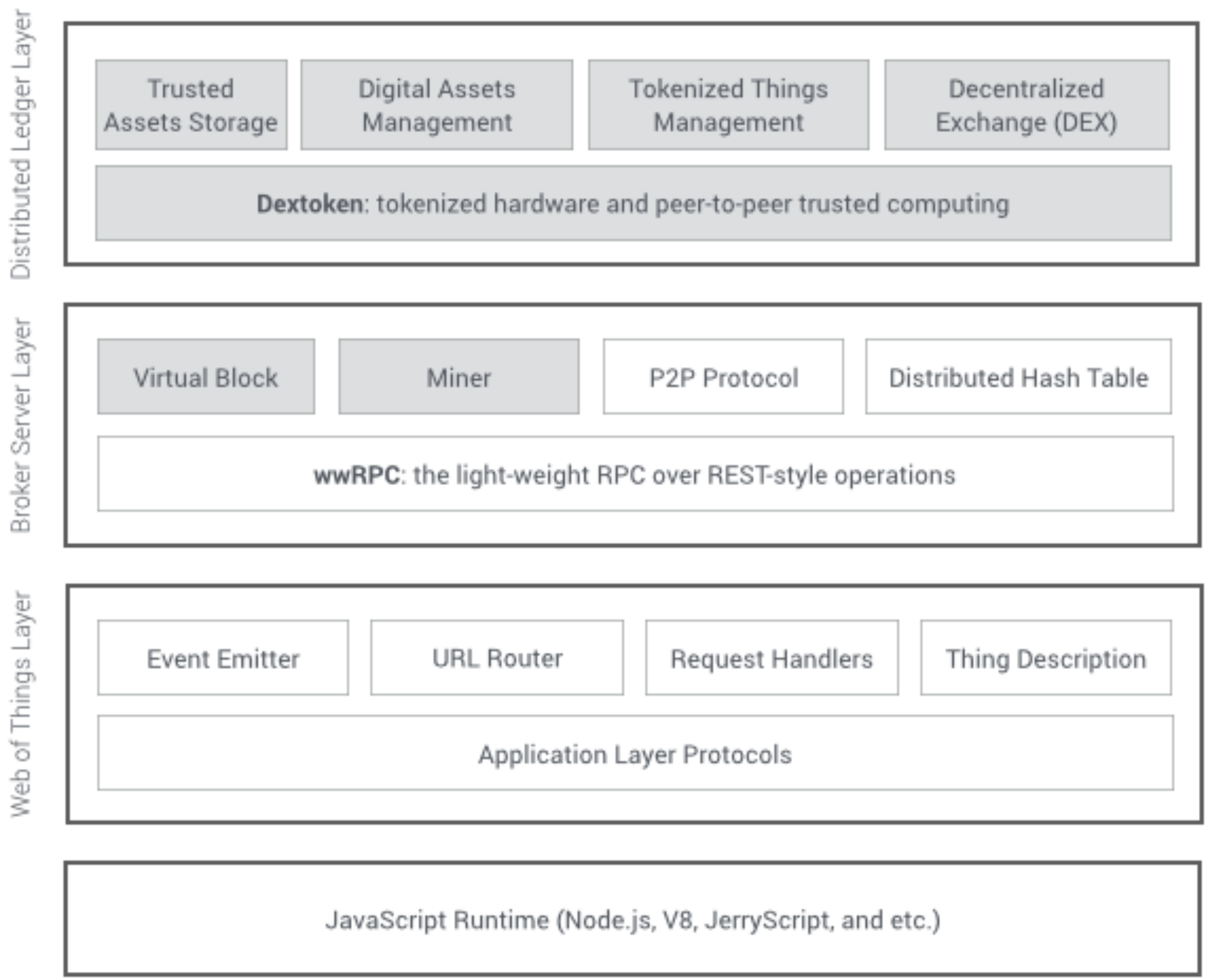
- The dataflow blockchain
- The Blockchain OS for IoT
- The Hybrid blockchain for IoT
- Decentralized AI

FLOWCHAIN

Blockchain OS, #2 of 4

FLOWCHAIN

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



Flowchain OS runs **Everywhere**

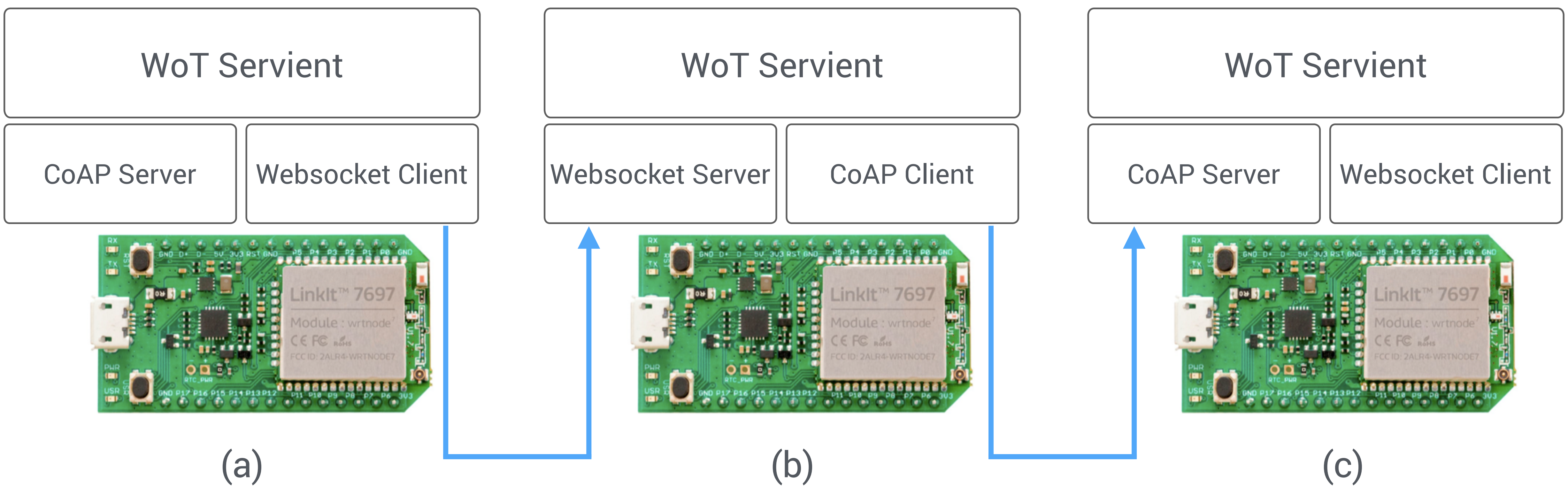
Dapps	Dapps	Dapps	JavaScript
RPC & DHT	RPC & DHT	RPC & DHT	JavaScript
Thing (WoT)	Thing (WoT)	Thing (WoT)	JavaScript
WebSocket / CoAP	WebSocket / CoAP	WebSocket / CoAP	JavaScript
Node.js 0.12	JerryScript	Node.js 4.4+	
OpenWRT (Linux)	FreeRTOS	MacOS	
MIPS Processor	ARM Cortex-M4	Intel Core 2	
580MHz 128MB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

FLOWCHAIN

The Broker Server Layer

FLOWCHAIN

- A WoT Servient comprises of client and server combinations.



SIGBED Review (ISSN: 1551-3688)
Special Interest Group on Embedded Systems

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

Content:

Editorial Board:

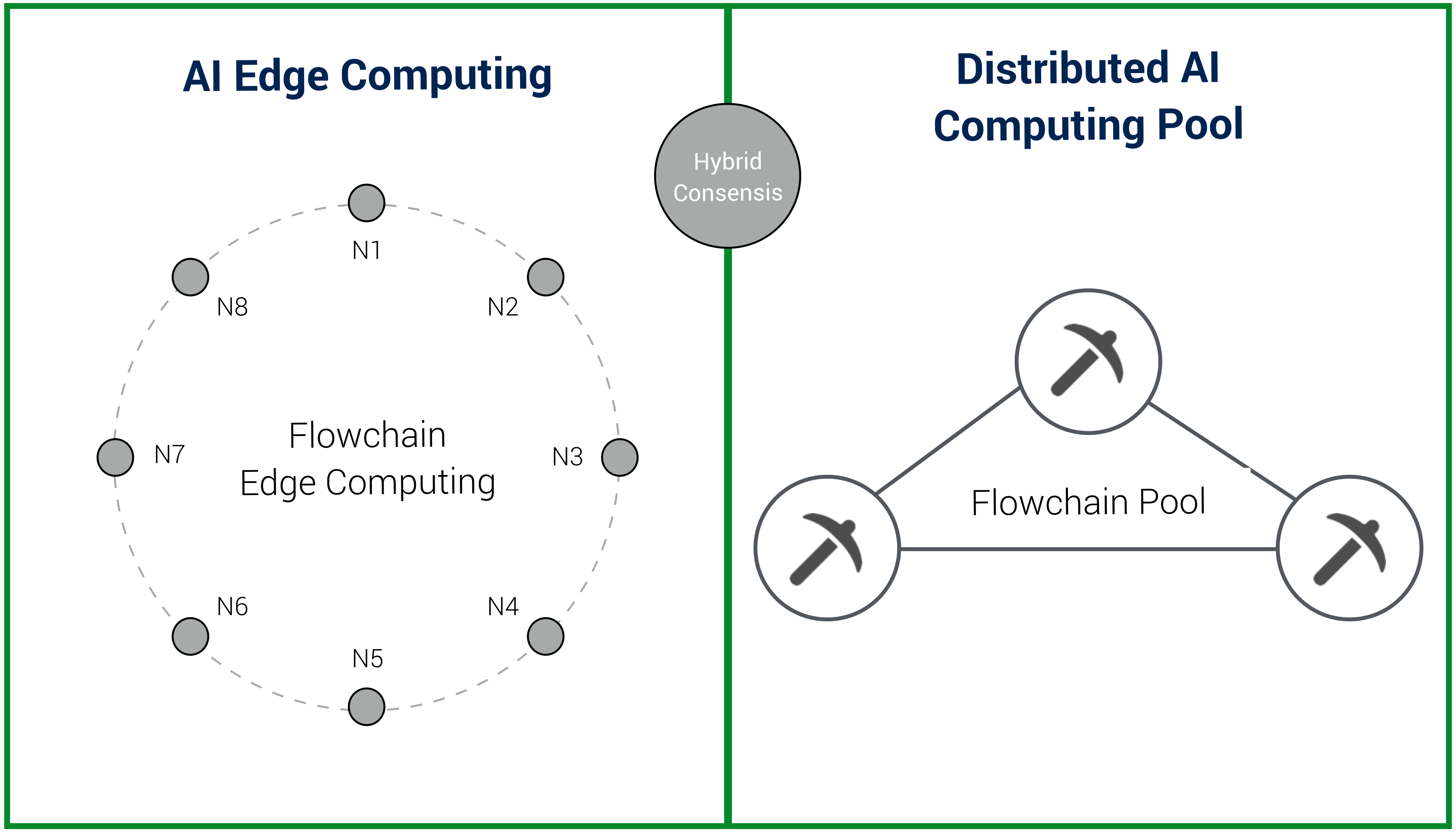
The Flowchain Insides

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

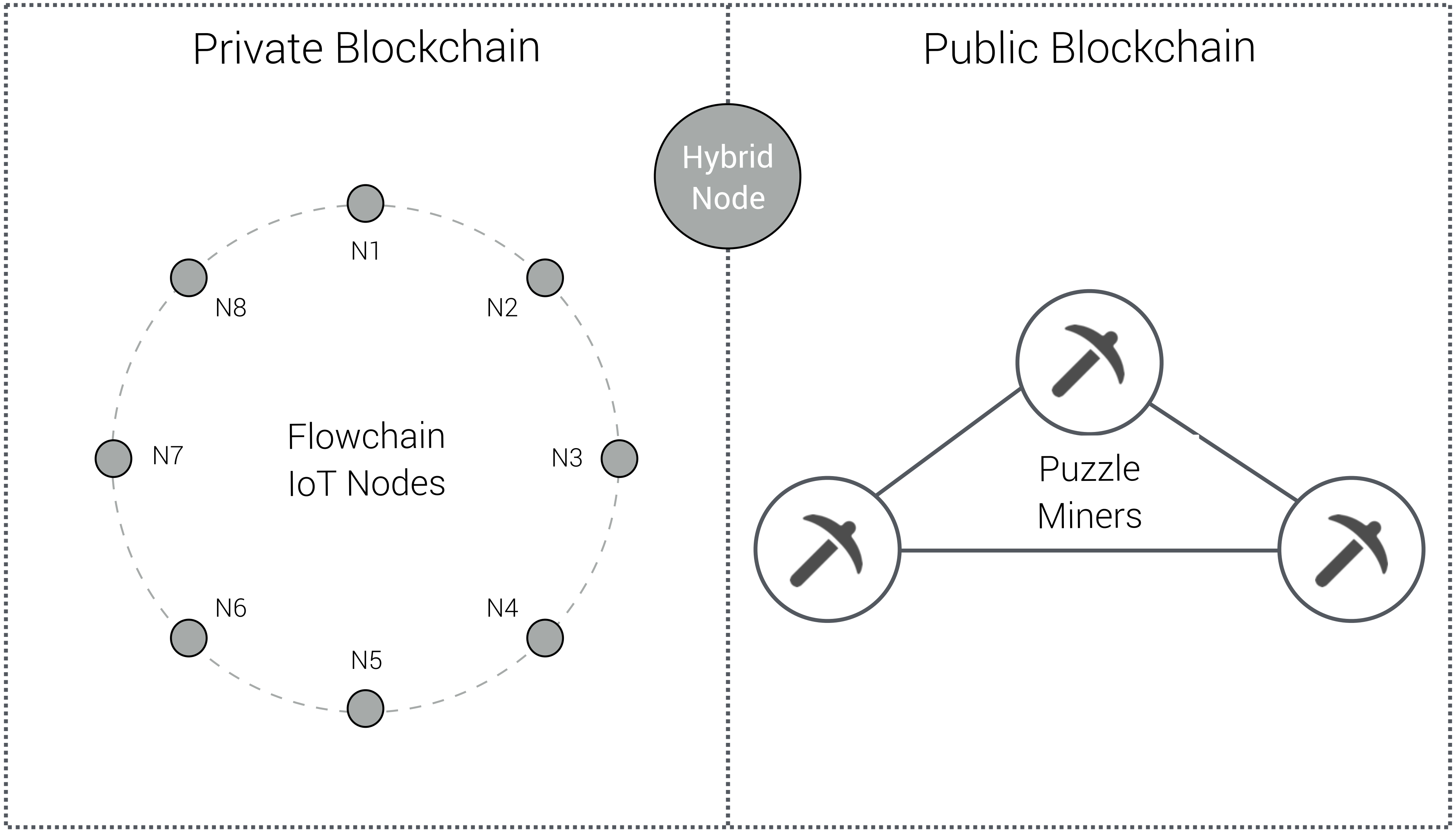
FLOWCHAIN

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 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.

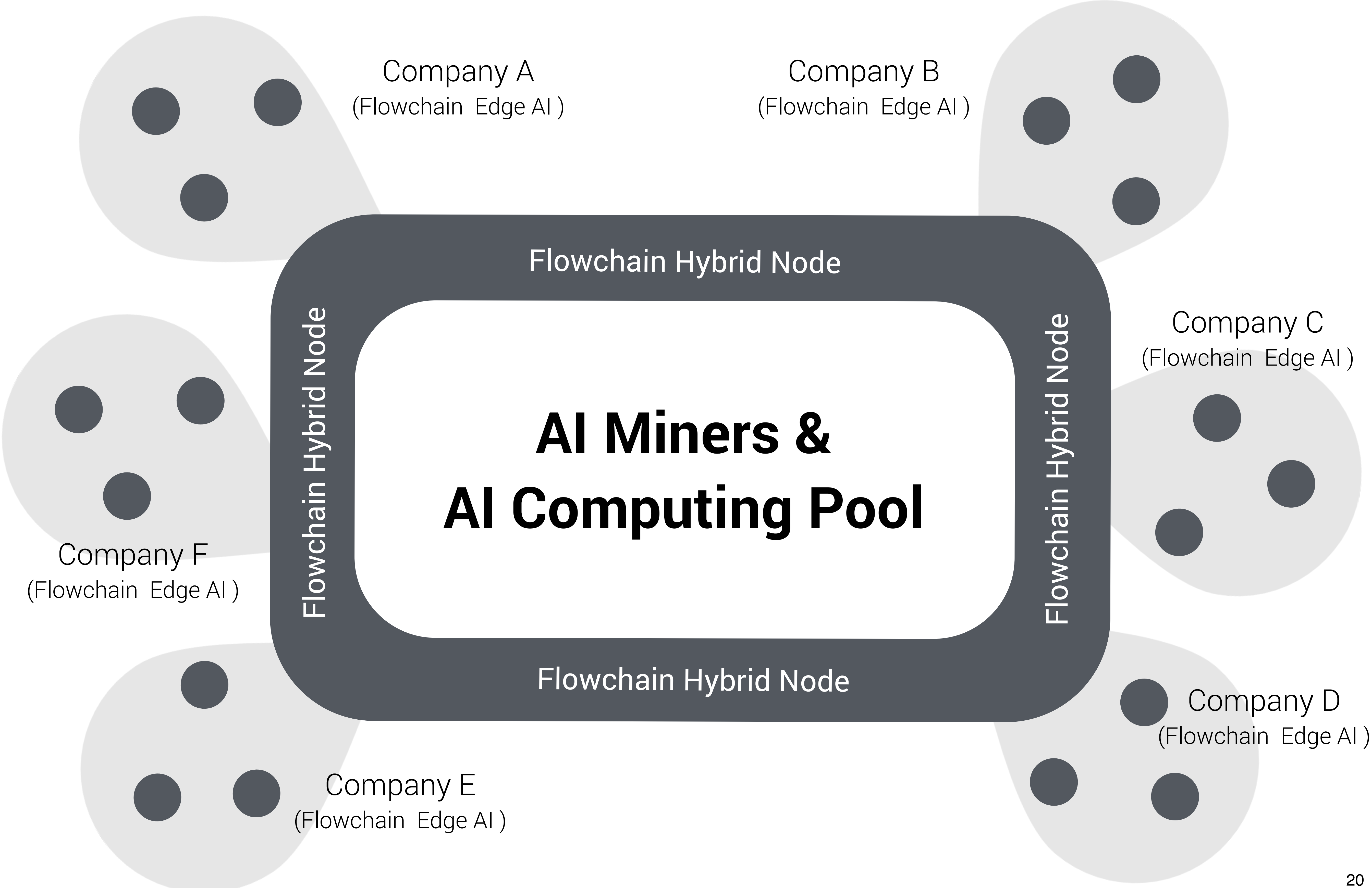


The Flowchain Insides

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

FLOWCHAIN

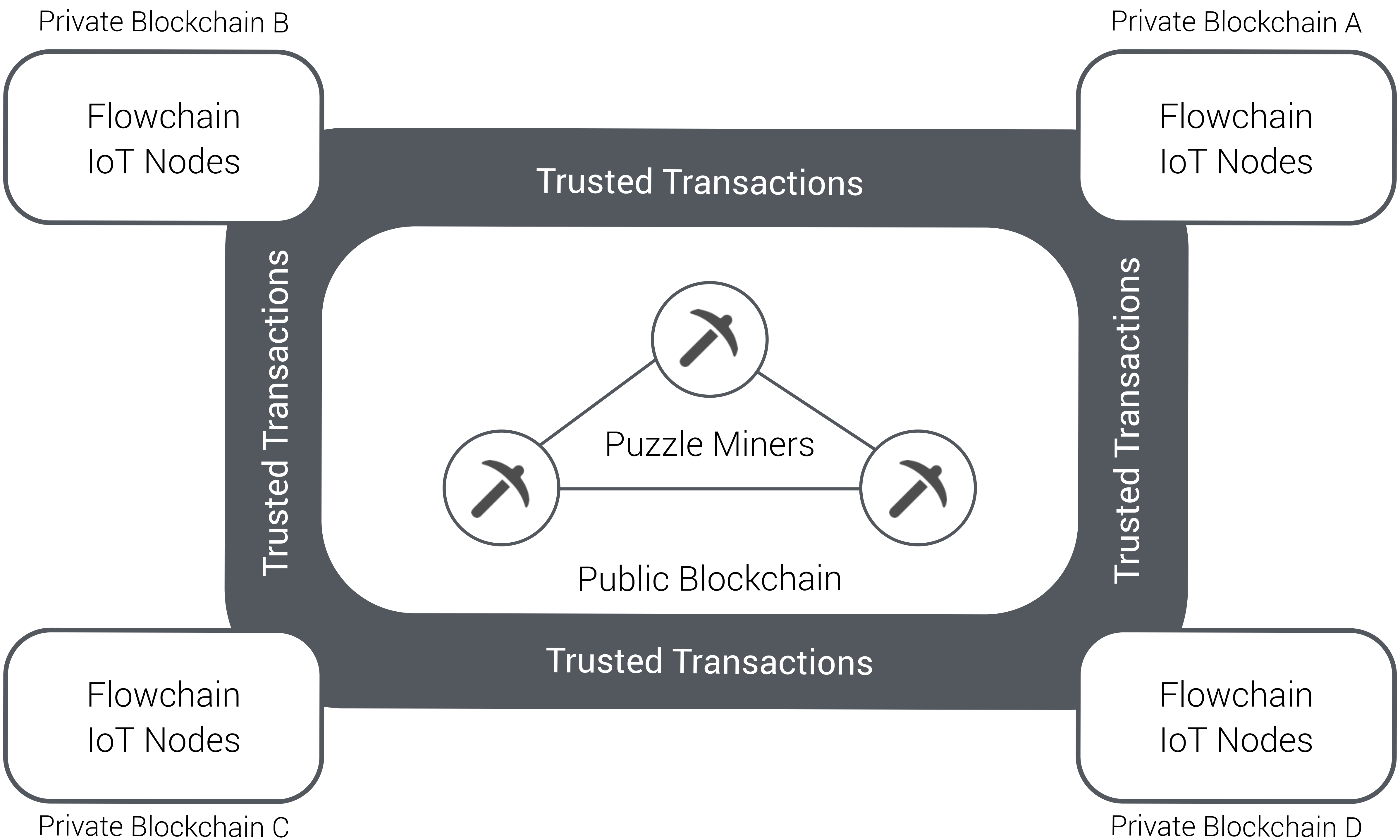
Decentralized AI, #4 of 4



Flowchain

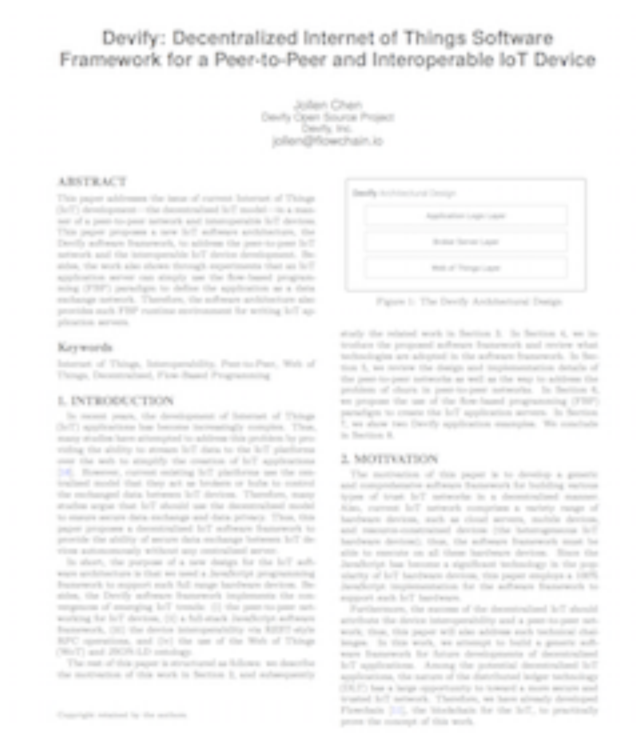
Pseudonymous Authentication

IoT Blockchain + AI over **Pseudonymous Authentication**



Academic Papers

FLOWCHAIN


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

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

Jollen Chen

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

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

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**.

FLOWCHAIN

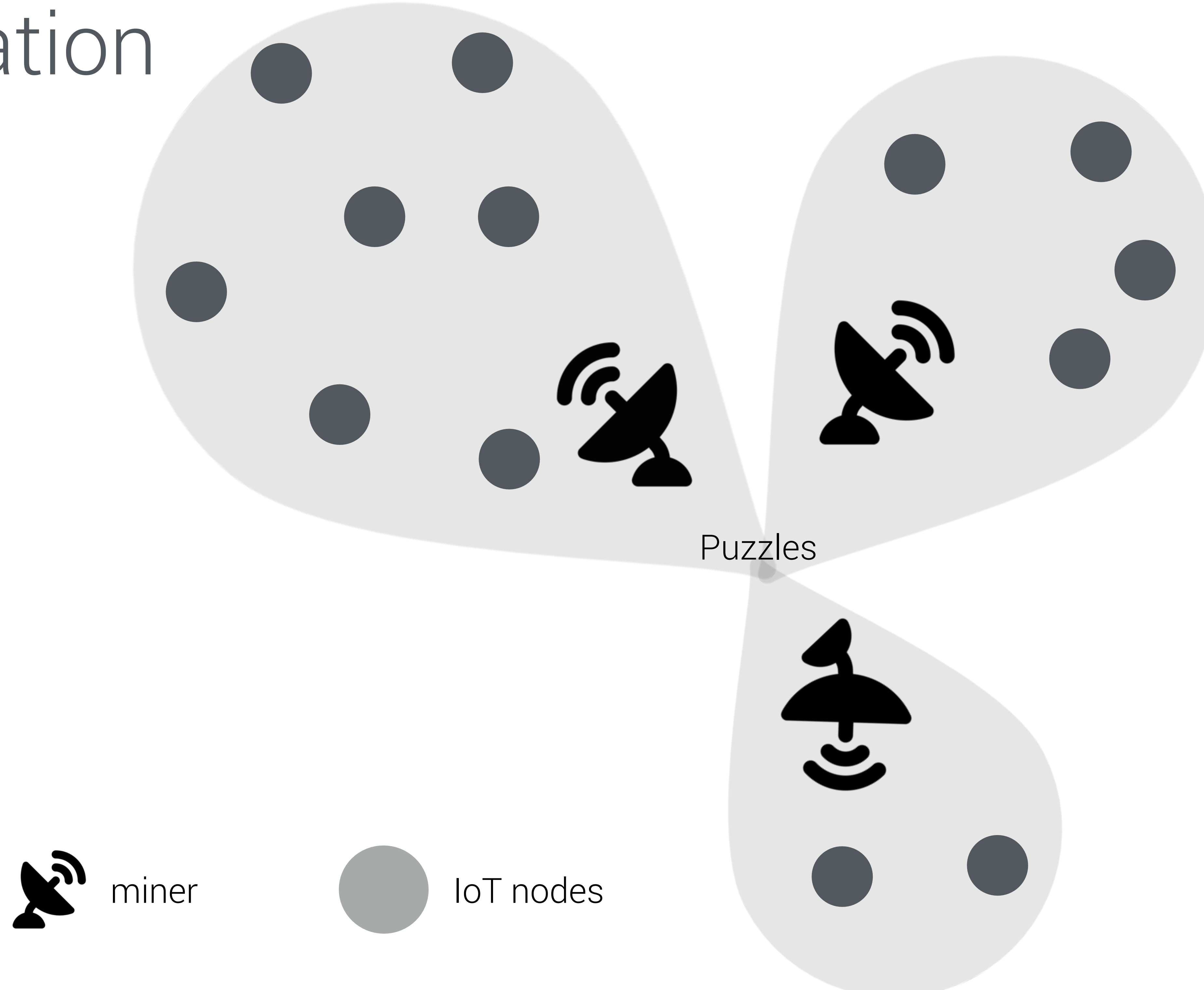
Private Blockchains

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

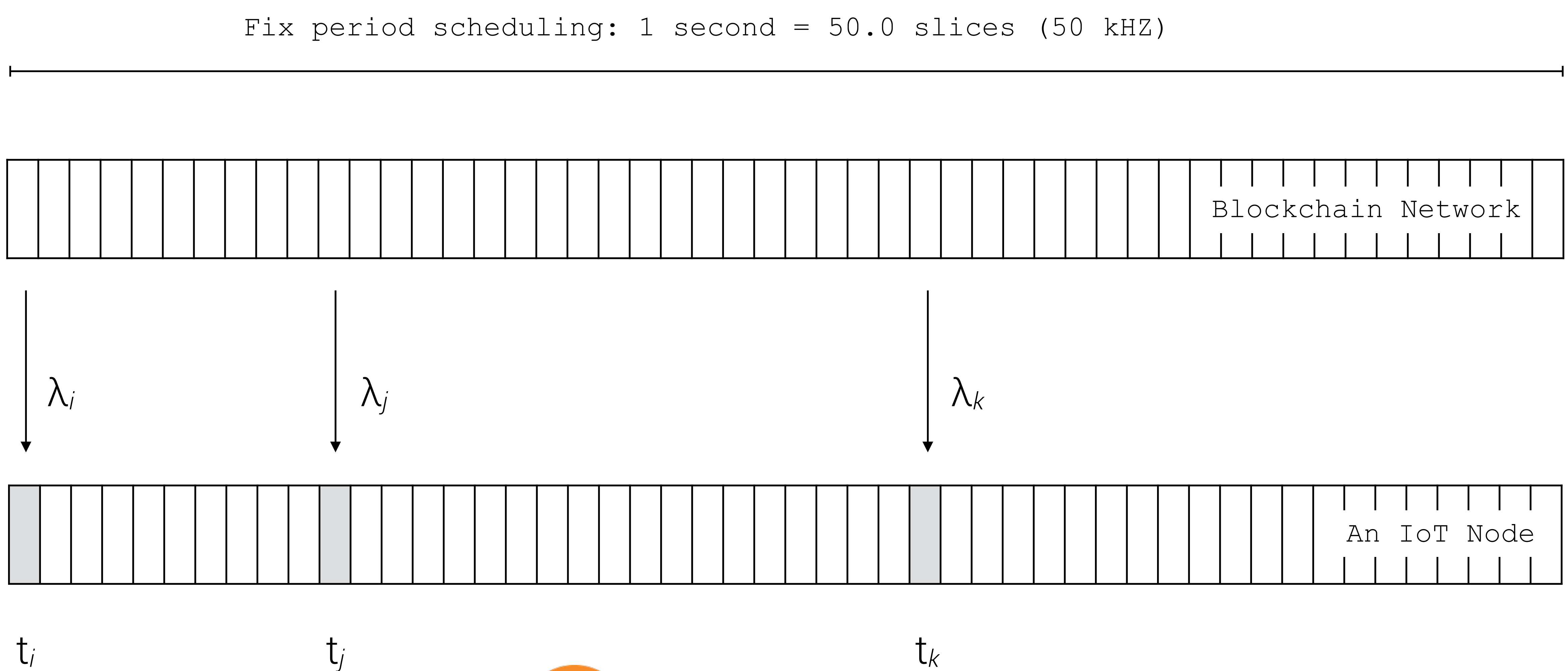
Pseudonymous authentication can replace the PKI to enable a fast authentication



FLOWCHAIN

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

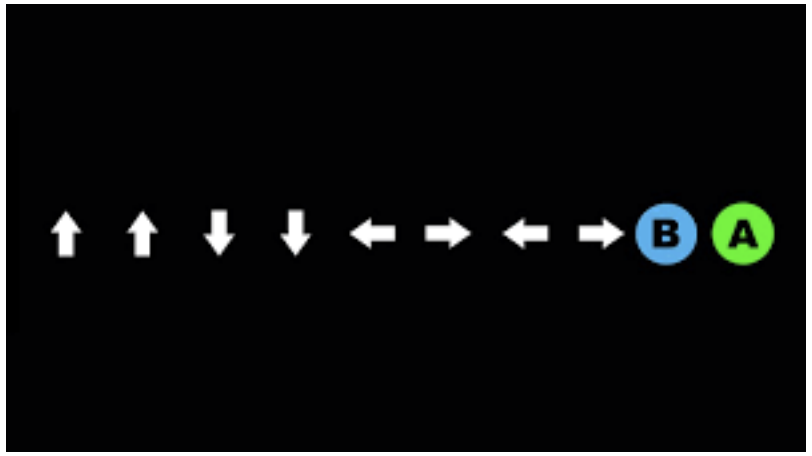
The IoT node was pseudonymously authenticated to submit transactions at (ti,tj,tk).

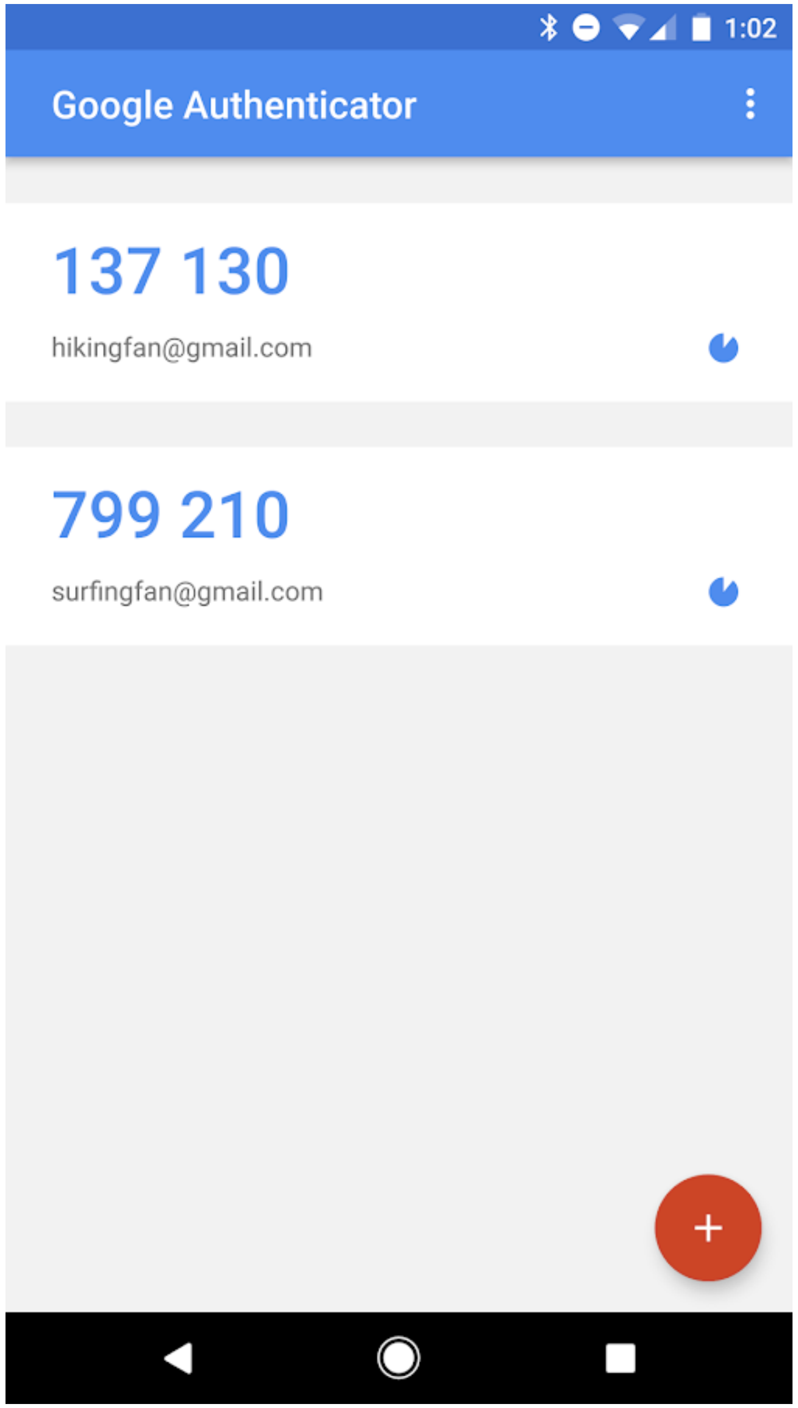


FLOWCHAIN

λ

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





FLOWCHAIN

FLOWCHAIN

```
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;
}
```

```
/**
 * The lambda value has to be unique, truly ramdom, 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;
};
```

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

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*

```
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.

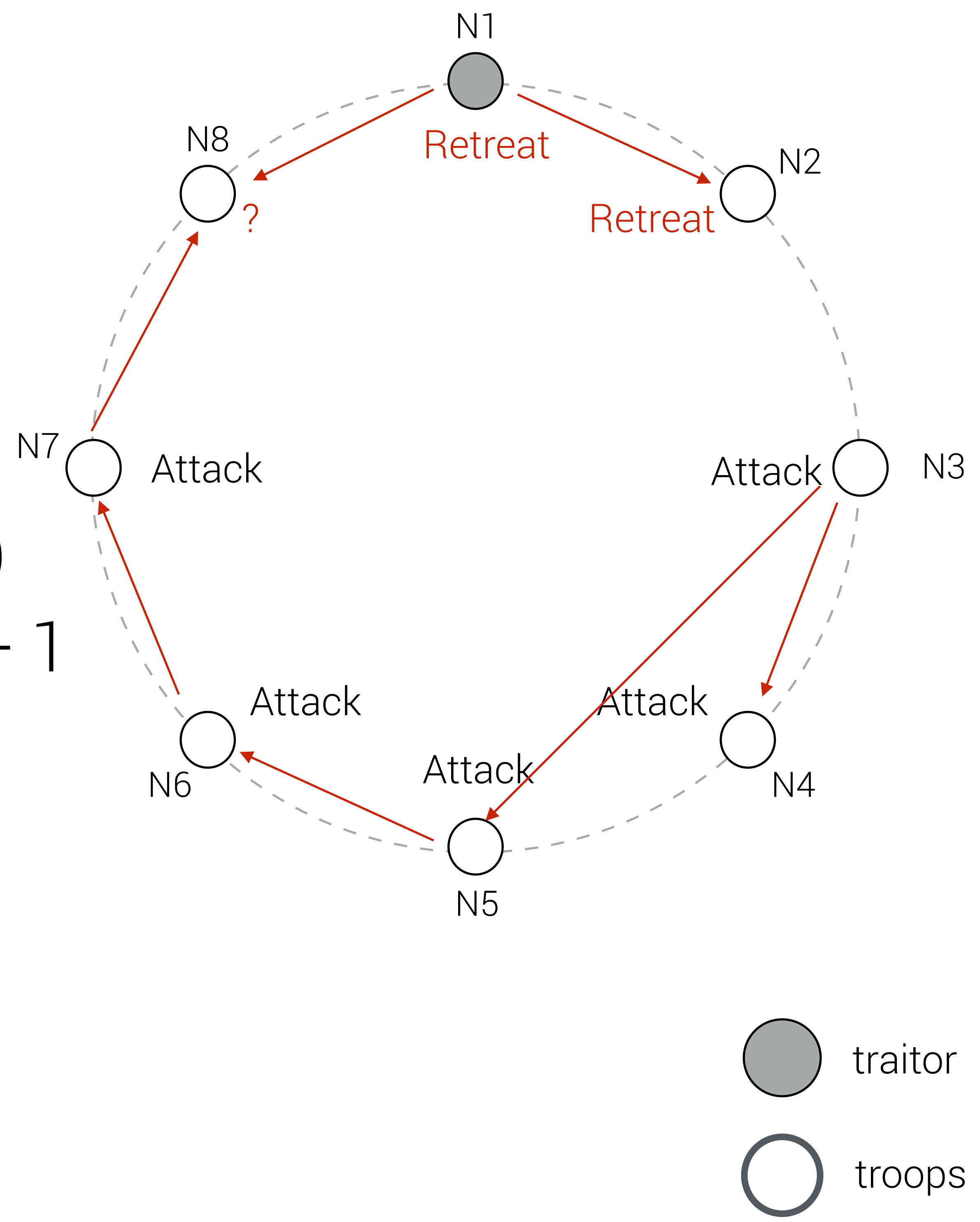
1. The trusted user $\mathcal{U}i$ produces a message or receives a message from another user through the p2p network; formally, let $\mathcal{M}$ be this message
2. The trusted user $\mathcal{U}i$ has the keypair (sk_i, pi_i); let $\mathcal{S}ign$ be the signature function
3. Let $\mathcal{T}i$ be the 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

Byzantine Fault Tolerance

FLOWCHAIN

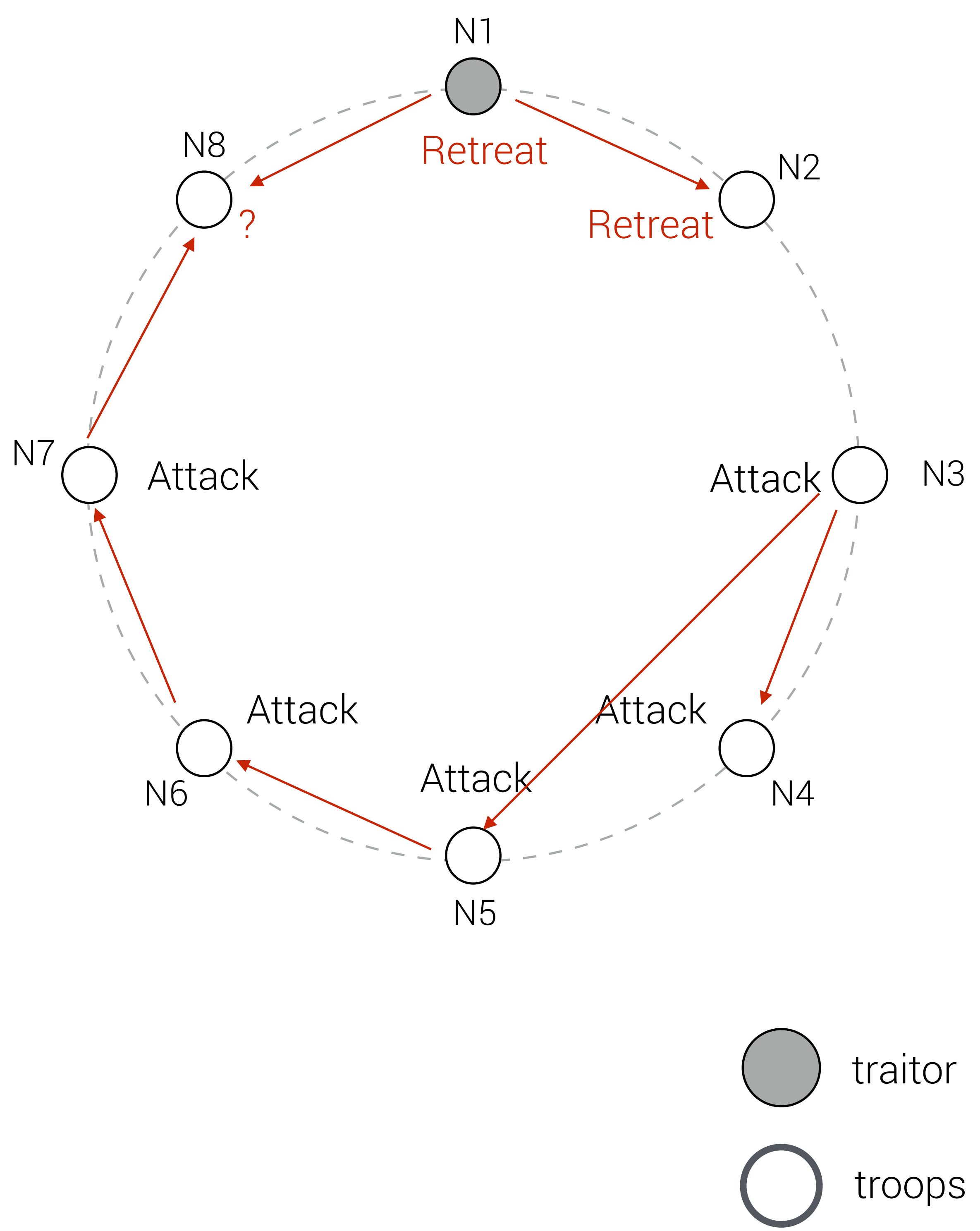
- **n** = 8
- **π** = 1
- $n > 3\boldsymbol{\pi} + 1$
- for n in [N1..N8)
  $f_{conn}(n) > 2\boldsymbol{\pi} + 1$



Flowchain BFT

FLOWCHAIN

- **n** = 8
- **π** = 1
- n >= **π** + 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

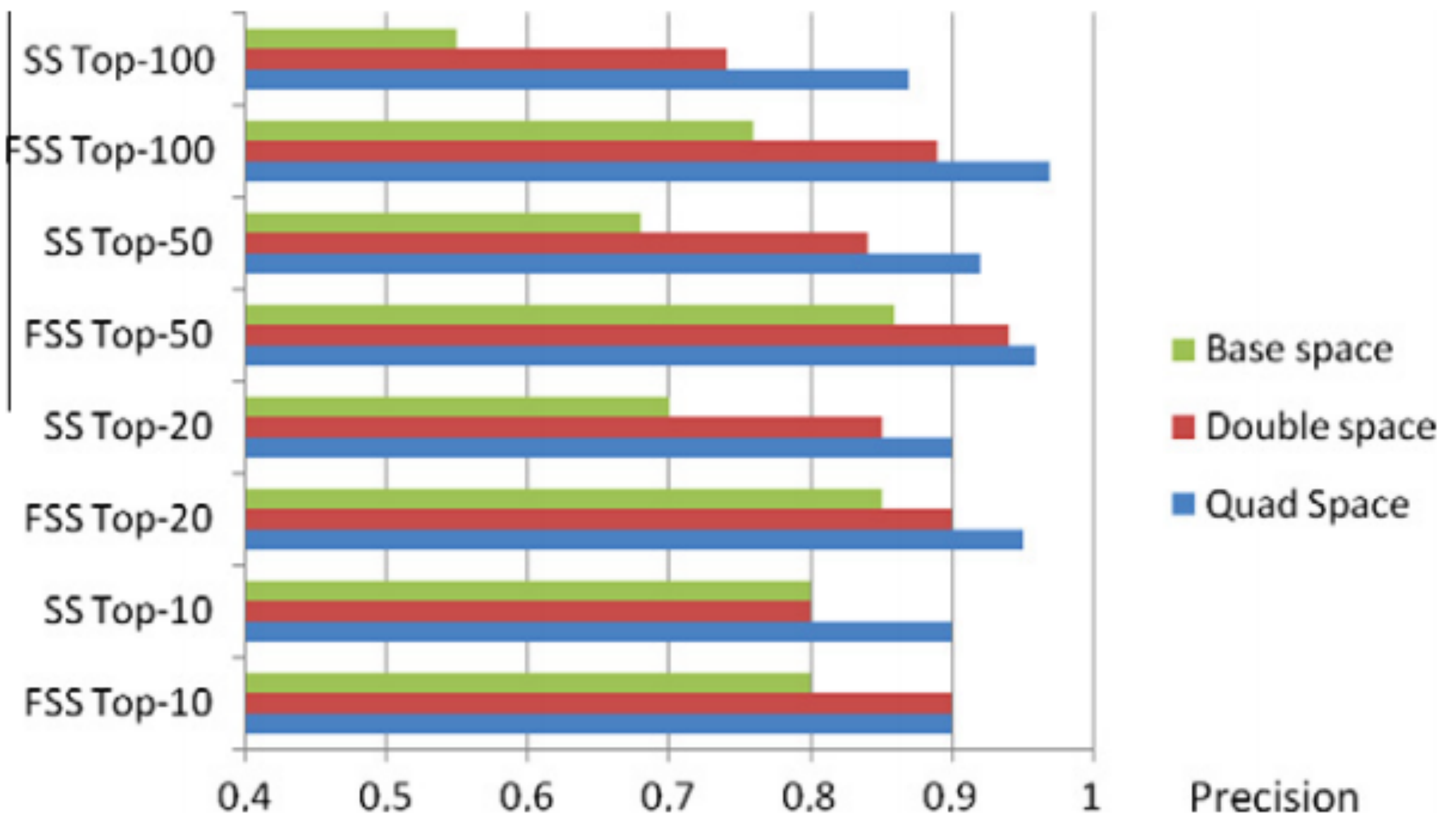


Fig. 10. Top-*k* Precision with increasing space in Trials 5.

基於 BFT 的共識算法

	Dolev	Fekete	FCA	CCA	Flowchain BFT	Brooks-Iyengar
Maximum faulty PEs	N/3	N/4	N/3	N/3	N/2	N/3
Complexity	Nπ	N/A	O(	N/A	O(	O(
Order of network bandwidth	O(N)	O(	O(N)	O(	O(N)	O(N)
Convergence rate	1/(N-2π-1)	1/((N-2π)/π)	2π/N	π/N	2*accuracy	2π/N

Trust and Anonymity

	Public	Private
Permissioned	PoS, DPoS Kafka	PBFT, SBFT Multi-signature
Permissionless	PoW PoET	**FlowchainBFT** FBA, Quantum

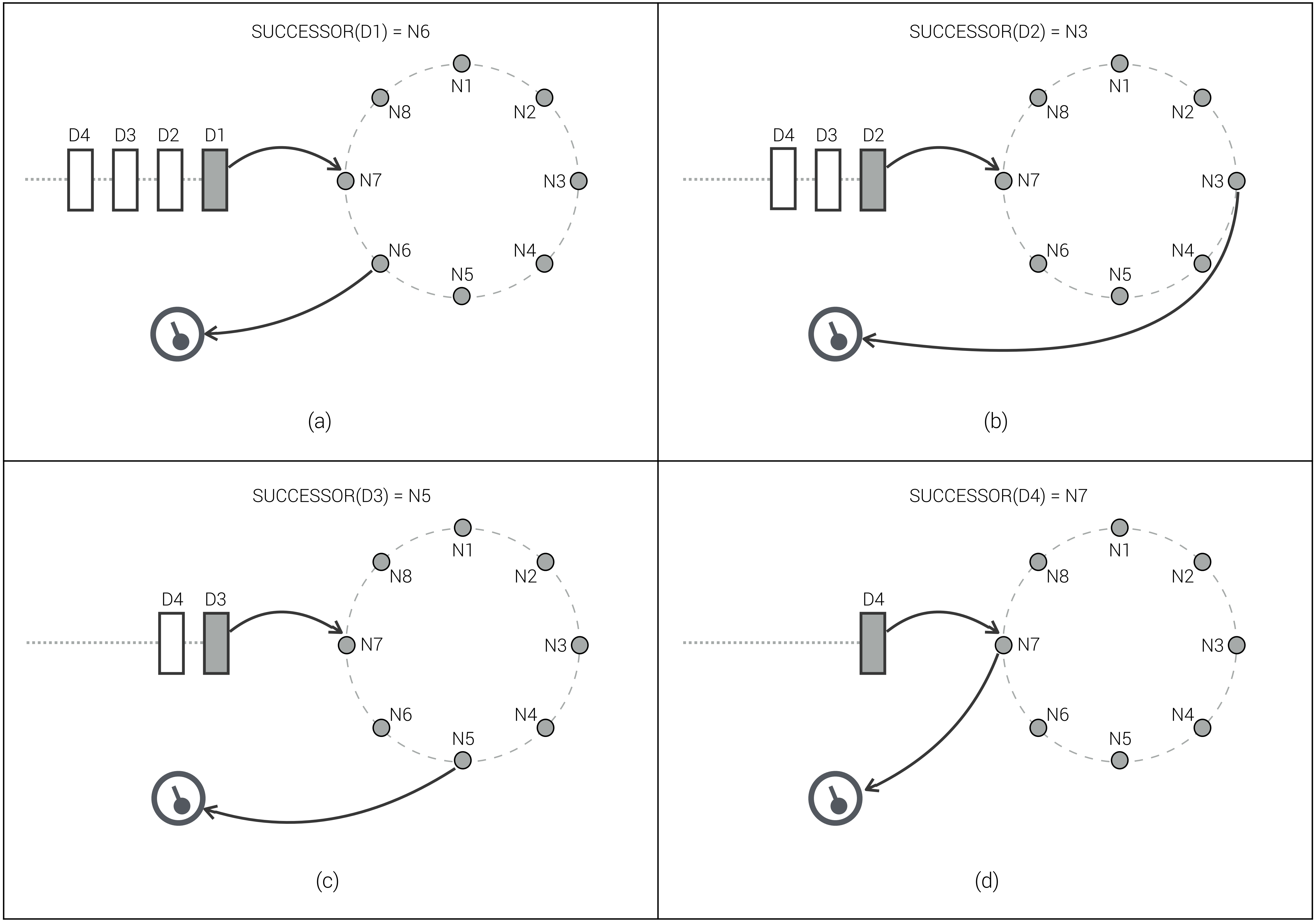
Trust

Anonymity

Source: https://flowchain.co

Flowchain

Submit Transactions

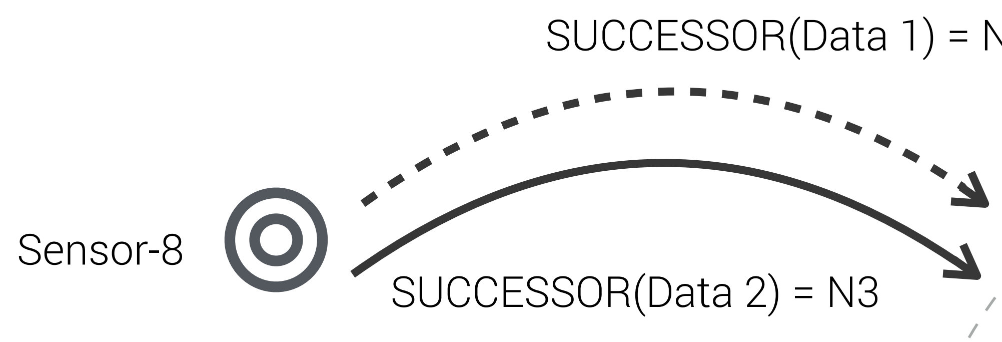

SUCCESSOR(D1) = N6
N1
N2
N3
N4
N5
N6
N7
N8
D4
D3
D2
D1
(a)
SUCCESSOR(D2) = N3
N1
N2
N3
N4
N5
N6
N7
N8
D4
D3
D2
(b)
SUCCESSOR(D3) = N5
N1
N2
N3
N4
N5
N6
N7
N8
D4
D3
(c)
SUCCESSOR(D4) = N7
N1
N2
N3
N4
N5
N6
N7
N8
D4
(d)

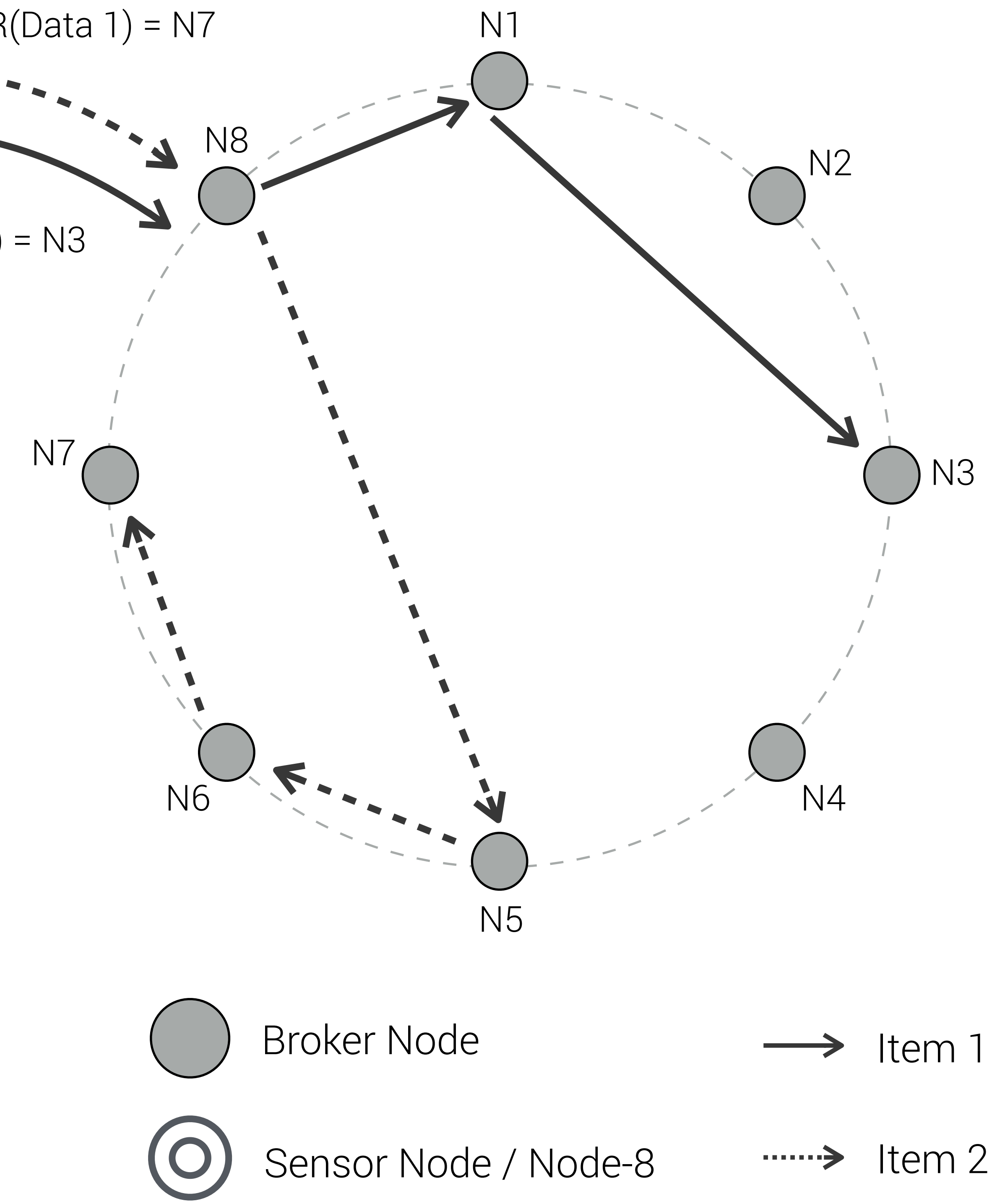

Flowchain Node
Endpoint Node

FLOWCHAIN

Flowchain P2P Dataflows

FLOWCHAIN





- 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

FLOWCHAIN

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

```
HDATA = SHA1( data + timestamp + ramdom )

SUCESSOR( HDATA ):
    Lookup the successor node in the DHT
```

Generating Transaction ID

FLOWCHAIN

- Use SHA256, SHA1, and Double SHA256
- The $\mathbf{H}_{DATA}$ hash is generated by the p2p network

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

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

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

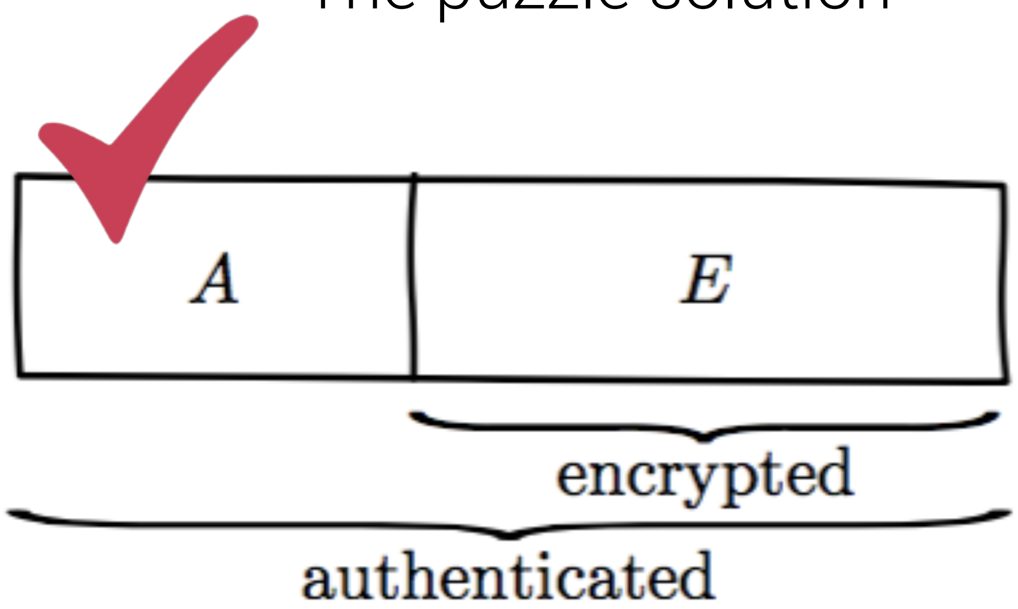
Data Transactions

FLOWCHAIN

- **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 - SUCCESSOR($\mathbf{H}_{DATA}$)
  - Step 3: Send [$\mathbf{H}_{DATA}$, λ] 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

Authenticated Encryption with Associated Data (AEAD)

The puzzle solution



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.

硬件代币化

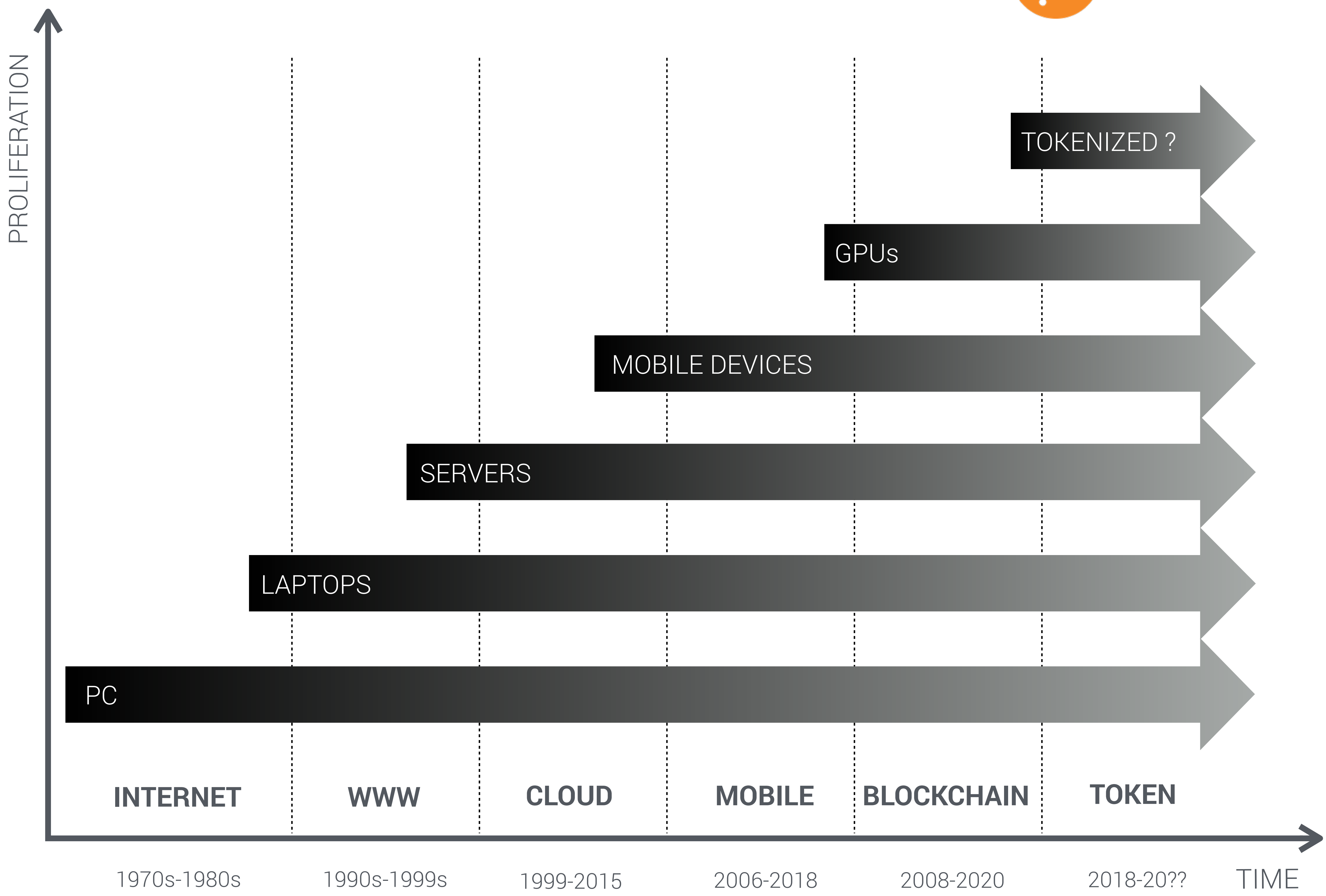
Coverstory Interview by Forbes Magazine, 2013

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.

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.

FLOWCHAIN


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

From Hardware to Tokenized Hardware

Hardware v.s. Tokenized Hardware

Hardware

- Tangible assets

Tokenized Hardware

- 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

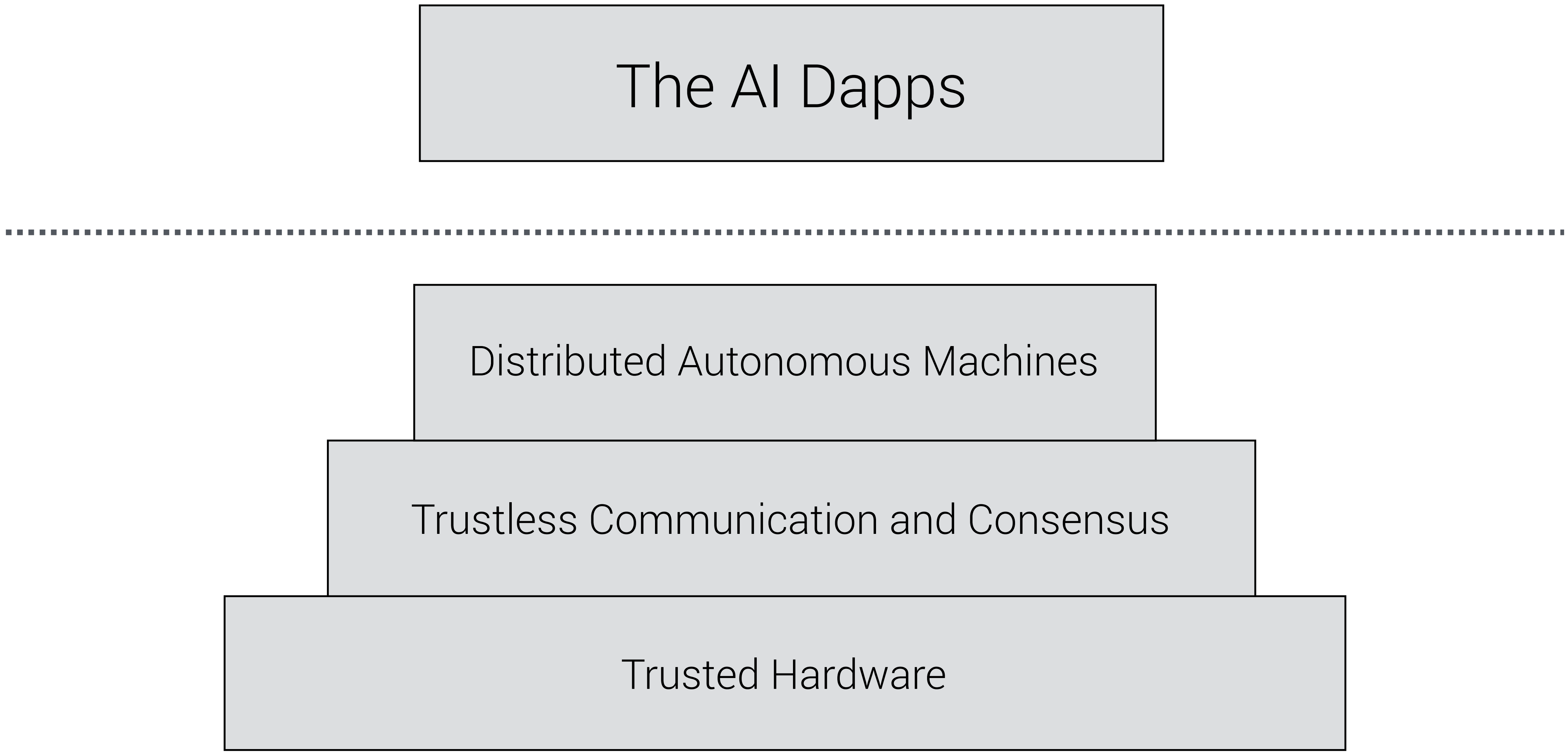
Conclusions

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



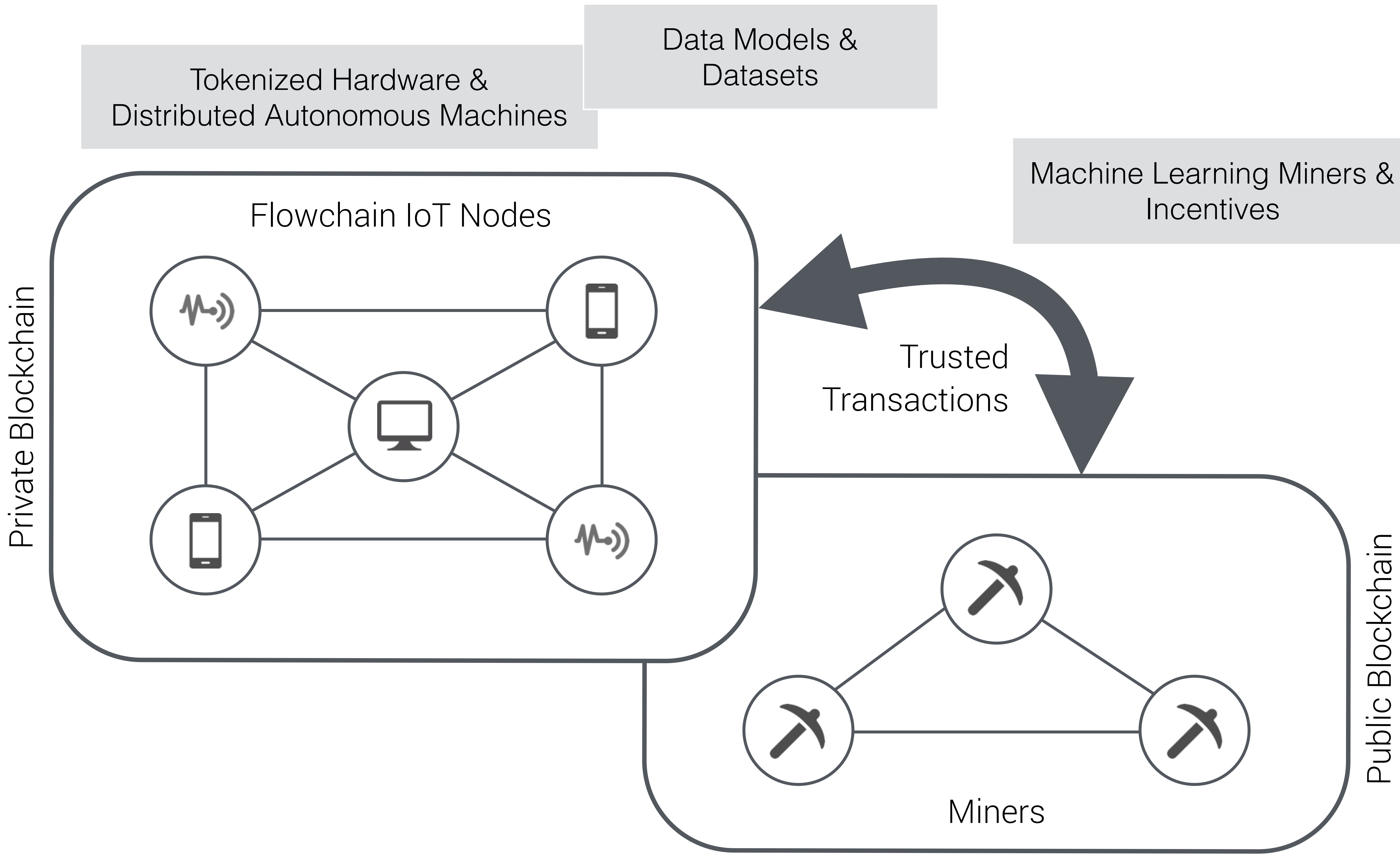
Flowchain underlying layer: Tokenized Hardware + DAM

FLOWCHAIN

	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 uppermost layer: AI over IoT Blockchain

FLOWCHAIN



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

FLOWCHAIN

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

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

Contact **jollen@flowchain.io**

WeChat **jollentw**