Flowchain

Whitepaper

Version: 3.0 Update: 2019.03.03

FLOWCHAIN

A distributed ledger for peer-to-peer IoT networks and real-time data transactions

Jollen Chen, Founder & CEO

jollen@flowchain.io

https://t.me/jollenchen

https://flowchain.co

Index

A Introduction

Abstract

This paper describes the Flowchain distributed ledger technology (DLT), the Flowchain digital assets (FLC), and the Flowchain IoT solutions (referred to as “products and services”). Developers, users, and enterprises should pay the products and services in FLC; further, they can pay the transaction fees to block producers (referred to as “miners”) on the Flowchain hybrid blockchain network in FLC.

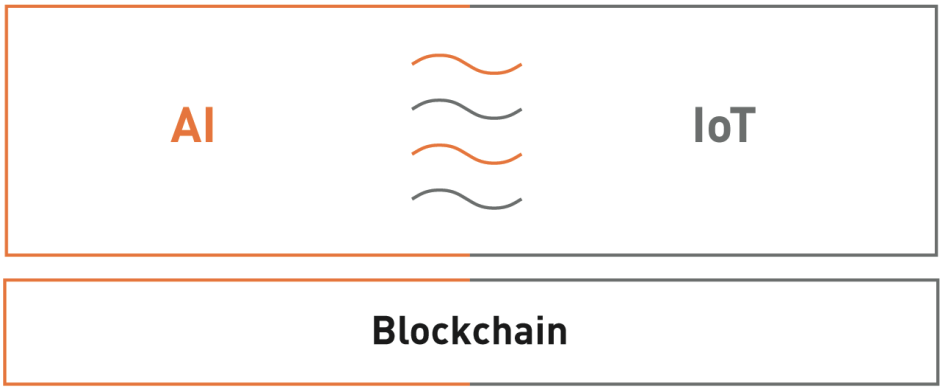
Based on Flowchain innovative technologies, Flowchain’s IoT solutions aim to provide a Data 2025 Ready total solution to the enterprises. By the year 2025, more than 150B IoT devices will be connected across the world and most of them will act in a real-time manner. However, current existing IoT technologies do not provide such real-time capabilities. By adopting Flowchain IoT solutions, the enterprises can fill the technology gaps.

Notably, the technology of Flowchain DLT and IoT solutions was built from the ground up to meet the needs of IoT. Flowchain’s technologies are supported by four peer-reviewed papers. Two reviewed papers are published on ACM publications.

In summary, Flowchain is ready for Data 2025. The Flowchain IoT solutions comprise multiple private blockchains, and a public trusted blockchain, such an architecture is called Flowchain hybrid blockchain architecture. The private blockchains provide an Edge Computing environment to ensure better real-time computing capabilities. Generally, a a large amount of data are transferred from the endpoint (the IoT devices) to the public cloud. However, the public cloud can not ensure the real-time computing

due to the limited network bandwidth and the long distance of data transfer. The enterprises can benefit from Flowchain hybrid blockchain with the edge computing solutions.

Flowchain - A new blueprint for the future of IoT and AI



【Figure 1】

"Artificial Intelligence (AI)" aims to continuously provide huge amounts of information to computers, allowing them to develop "Machine Learning" through statistical and probabilistic analysis methods, and then through "Artificial Neural Networks" to shape and achieve "Deep Learning"; the ultimate goal is to create a computer that can think independently like human beings.

Moreover, "Internet of Things (IoT)," proposed by Kevin Ashton, director of the MIT Auto-ID Center in 1998, aims to connect real-world objects to the Internet through data capture and communication capabilities. The computer detects, identifies, manages and controls the device, and has broad market and application prospects in transportation and logistics, medical field and smart devices.

Flowchain's vision is to adopt the "blockchain" technology and use it to create great value by connecting the two areas of "Artificial Intelligence" and "Internet of Things" that are not highly correlated and highly specialized. What Flowchain wants to build is not

just a blockchain technology, but a new blueprint for the future of IoT and artificial intelligence about a revolution of "AI + IoT."

Flowchain IoT blockchain concept

The IEEE released a newsletter in January 2017 to analyze the technical challenges of the IoT Blockchain[1]. It mentioned that from the perspective of IoT Architecture, there exists several significant technical challenges of the IoT Blockchain. In conclusion, a "Decentralized IoT Architecture" will be the opportunity to address such technical challenges.

When the Blockchain technology is applied to the IoT architecture, the "Decentralized" IoT architecture is required to become a standard discussion topic. However, what benefits does this decentralized architecture bring to IoT applications? The most critical issue is Data Privacy. When people transfer IoT data to a specific IoT Platform, they lose control of valuable data ownership, usage rights, and storage.

Data is the most important asset of the Internet of Things system. Therefore, in view of the nature of the regression blockchain, IoT Blockchain can provide Data Privacy solutions for existing IoT network architectures, and at the same time, Data Security can be improved through the introduction of Trust mechanism. Data Privacy and Data Security are the major two issues of the IoT architecture, and also have an intersection of Semantic Web's appeals.

That is to say, from the perspective of application scenario, IoT blockchain technology does not solve the deep technical problems, but **provides the additional commercial value of Data Privacy and Trust for the existing IoT industry ecology**. Therefore, the reason why Flowchain needs to have a decentralized architecture is not for inventing a new technology, but the desire to create such additional business value.

---

[1] IoT and Blockchain Convergence: Benefits and Challenges, http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

From a technical perspective, how can we create a Decentralized IoT Architecture? At present, the most common view is to implement the IoT Network using Peer-to-Peer technology. The Flowchain project is a system that wants to build an IoT Blockchain in the same way as Peer-to-Peer Networking.

B Dilemma and Solution

Preliminary

The Edge Device in IoT is mainly based on "Sensor," which does not have enough computing power, because such sensors are usually constraint devices. Therefore, the future of data collected will be used as "Data Mining," or as a cultivating AI, developers must rely on additional "computing power" inputs.

At present, the source of computing power is mainly "Graphics Processing Unit (GPU)," also known as display core, visual processor, display chip or graphics chip, which is not only expensive but also expensive to operate. "Electricity" has always been the main reason for companies to stagnate and hinder the burgeoning development of related industries such as AI and IoT.

For such an industry dilemma, Flowchain proposes a solution called "Hybrid Blockchain" which is a combination of "Public Blockchain" and "Private Blockchain."

For such an industry dilemma, Flowchain proposes a solution called "Hybrid Blockchain" which is a combination of "Public Blockchain" and "Private Blockchain".

Industry Dilemma - "Computing Power" and "Electricity"

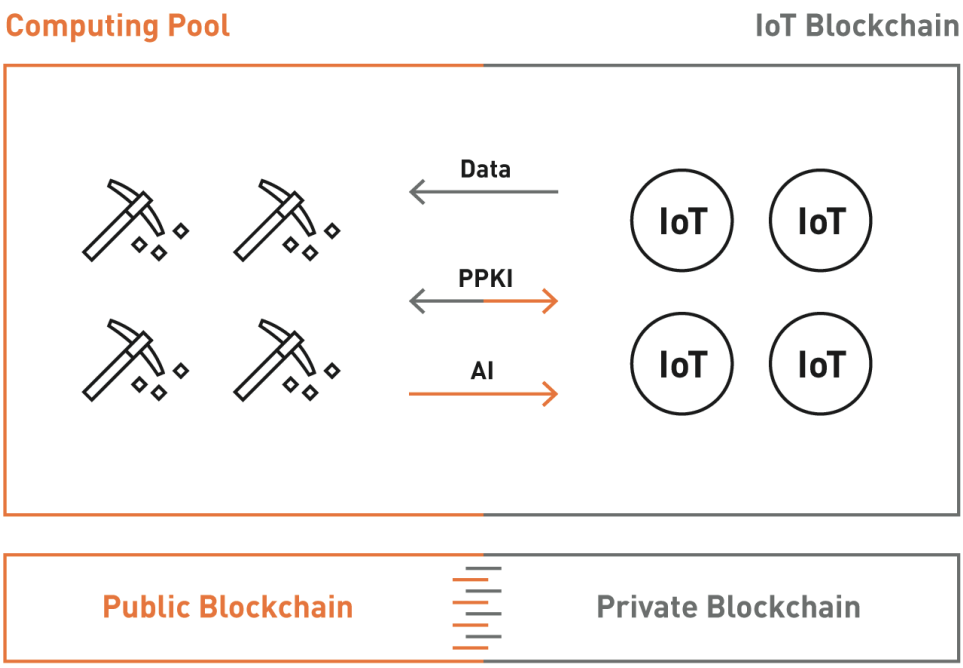
In recent years, the "Miner" trend brought about by the rise of Bitcoin; a social movement of global cryptocurrency mining has followed. The Flowchain looks at the largest computing network ever made – initially estimating that the miners scattered around the world can provide at least 88,000T of computing power. Instead of investing in a large capital for building and operating centralized computing power center, Flowchain proposes a second option – building a decentralized “computing and resource Pool” (referred to as “Computing Pool”) through the blockchain as the underlying technology; inviting miners scattered around the world to participante and share their "idle computing power" and “excess storage space” required by IoT and AI. In this way, developers who are doing "big data," "machine learning" or "Internet of Things" can enjoy the computing power and storage space in this decentralized computing and resource pool at a relatively low cost, forming a "distributed computing power and network storage platform and the business model.”

It is conservatively estimated that even if only 10% of the miners in the world are stationed, this computing and resource pool still has a huge computing power of 8,800 T; private companies which need to construct a centralized computing center to provide such computing power have to invest in a large amount of money to buy GPUs. Such cost is estimated - 38,000 GPUs (providing 100T of computing power) x 88 x 1,000 dollars (the price of a GPU) = about $3.3 billion. This figure has not yet included miscellaneous items such as "land acquisition fee", "factory construction fee" and "electricity fee"; saving such a huge amount of expenses will undoubtedly be a shot in the arm of AI and IoT and other related industries.

Private Blockchain – Flowchain

By developing exclusive chips and "Software Development Kit (SDK)," Flowchain allows IoT companies and developers to easily customize their products and services and build

their own IoT Blockchain on the Flowchain platform. The huge amount of data collected from the device will be passed back to the Flowchain computing and resource pool; the miner will provide the computing power to calculate the more intelligent "Inference Engine (AI)", and then push back to the IoT Blockchain to let the device AI Upgrade to become smarter and more efficient. This escalating positive cycle is the new blueprint portrayed by Flowchain - "The Fourth Industrial Revolution - AI + IoT Generation."



【Figure 2】

Compared with most IoT Blockchain, which emphasizes the connectivity technology of the device, Flowchain thinks that the key point is "Data Flow"; that is, Data is the "Flows" between the device and the computing and resource pool. The concept is also the origin of the Flowchain name - "Dataflow's Blockchain."

Real strength - action is the best proof

Compared to other blockchain projects, Flowchain officially launched the Token Sale program in 2018 after completing the preliminary research, development and prototyping phases.

【圖 3】

In the research phase, Flowchain has published several peer-reviewed academic papers listed below.

Research Paper

June 3, 2018 NEW
Download this paper

Flowchain Hybrid Blockchain research paper

Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks

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

https://flowchain.co/

June 25, 2017
Download this paper

The Devify framework research paper

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

In proceedings of the Workshop on Advances in IoT Architecture and Systems, June 25, 2017, Toronto, Canada.

https://flowchain.co/

May 29, 2017
Download this paper

The Flowchain framework research paper

Flowchain: A Distributed Ledger Designed For Peer-to-Peer IoT Network And Real-time Data Transactions.

In proceedings of the 2nd International Workshop on Linked Data and Distributed Ledgers, May 29, 2017, Portoroz, Slovenia.

https://flowchain.co/

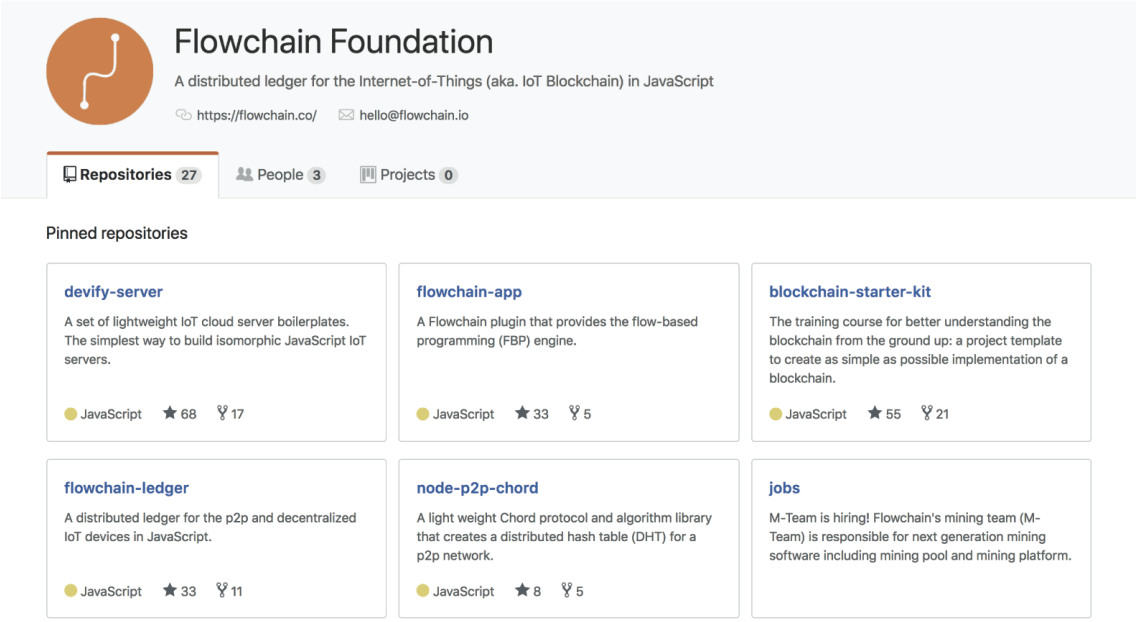
February 2, 2017
Download this paper

The tokenized hardware white

Tokenized Hardware: The New Crypto Innovation

https://flowchain.co/

【Figure 4】



【Figure 5】

In December 2018, the test network of Flowchain was officially launched. Since its inception, Flowchain has achieved the ideal blueprint step by step with practical action and real strength.

C Flowchain Architecture

To make the Flowchain platform more complete, and to build a sustainable blockchain ecosystem, Flowchain introduces the concept of "blockchain software and hardware integration." Besides, to create Flowchain Operating System, the underlying technology of Flowchain, we also take Taiwan's advantage of the hardware manufacturing industry and strategic alliance with the Electronic Manufacturing Services (EMC) vendor. This ecosystem works together to build a complete Flowchain platform.

The key to the Decentralized IoT

Is there a technical challenge to implementing a Peer-to-Peer (P2P) network in the IoT architecture? The goal of implementing P2P IoT Networking is to enable IoT Devices to establish a P2P communication topology. Such an implementation effort is a technical challenge. Technically, it may not be much difficult for IoT Devices to form a P2P network; however, if you go deeper into the technical details, you find much knowledge.

First, consider the application layer, IoT devices communicate with each other by application layer protocols, such as HTTP. Therefore, we need to be able to run an "Application Server" on the IoT device, that is, we must implement a "Programming Framework" before we can develop the Application Server on the IoT device. The Programming Framework mentioned here can be an IoT operating system or Middleware, but the main point is why P2P's IoT Networking uses the top-level application layer protocols; this is an interesting topic worth exploring.

Second, the consideration of heterogeneous hardware. Flowchain started with the creation of a Web of Things Framework [2]. The purpose of this software framework is to implement a development framework for IoT Application Server in JavaScript. With this framework, you can achieve two purposes:

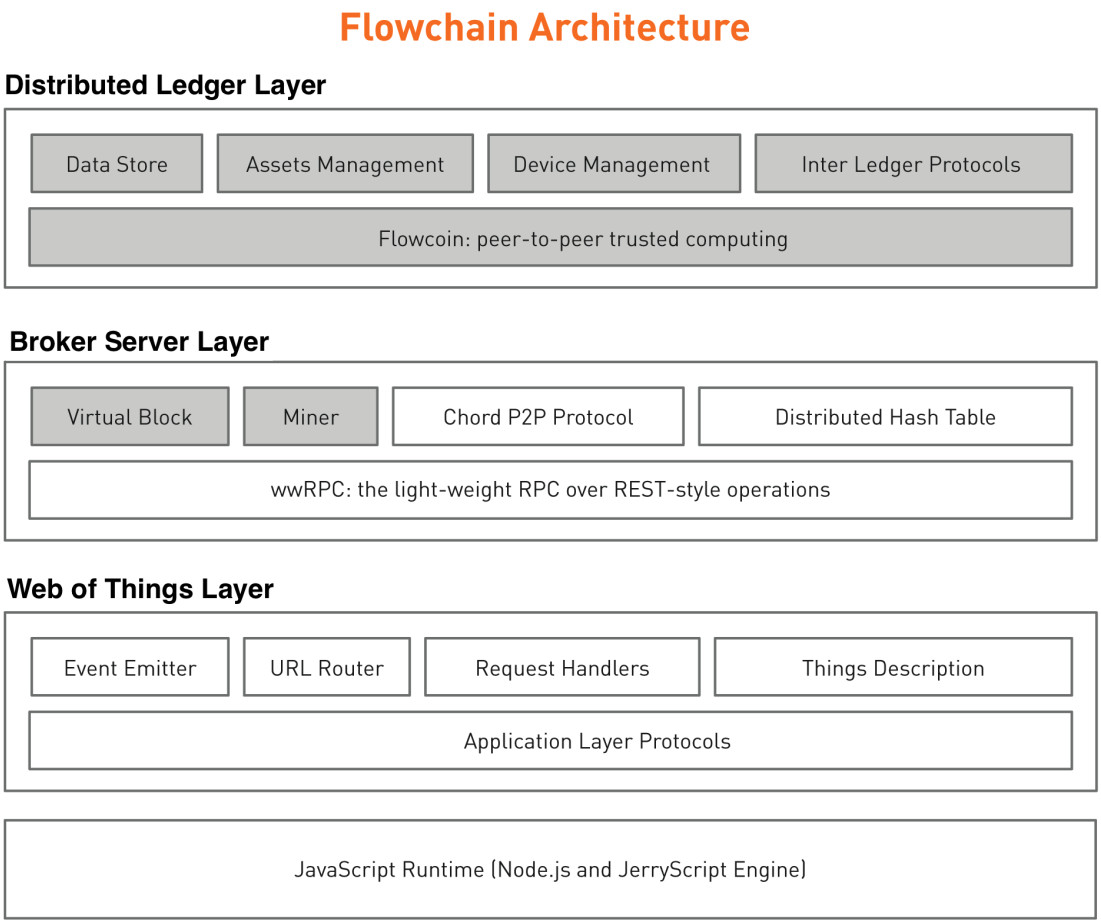
1. Can run this IoT Application Server on different IoT Devices

2. Abstraction of IoT Device to **Virtual Thing**

If the heterogeneous hardware has a JavaScript runtime, the IoT Application Server can be deployed and run on such hardware device. Because the open source community has introduced technologies such as Node.js and JerryScript, the idea is now highly feasible.

[2] Web of Things Implementations, https://www.w3.org/WoT/IG/wiki/Implementations

Software | Flowchain OS - the core technology of AI and IoT



【Figure 6】

Flowchain OS is the soul of Flowchain, and also the core technology of bridging computing pool and IoT Blockchain. Compared with other Blockchain projects which are built on the Ethereum open source blockchain platform. Flowchain chooses to build from zero. The new blockchain organization is shown above, and described from bottom to top -

- **JavaScript Runtime – The programming language of Flowchain**

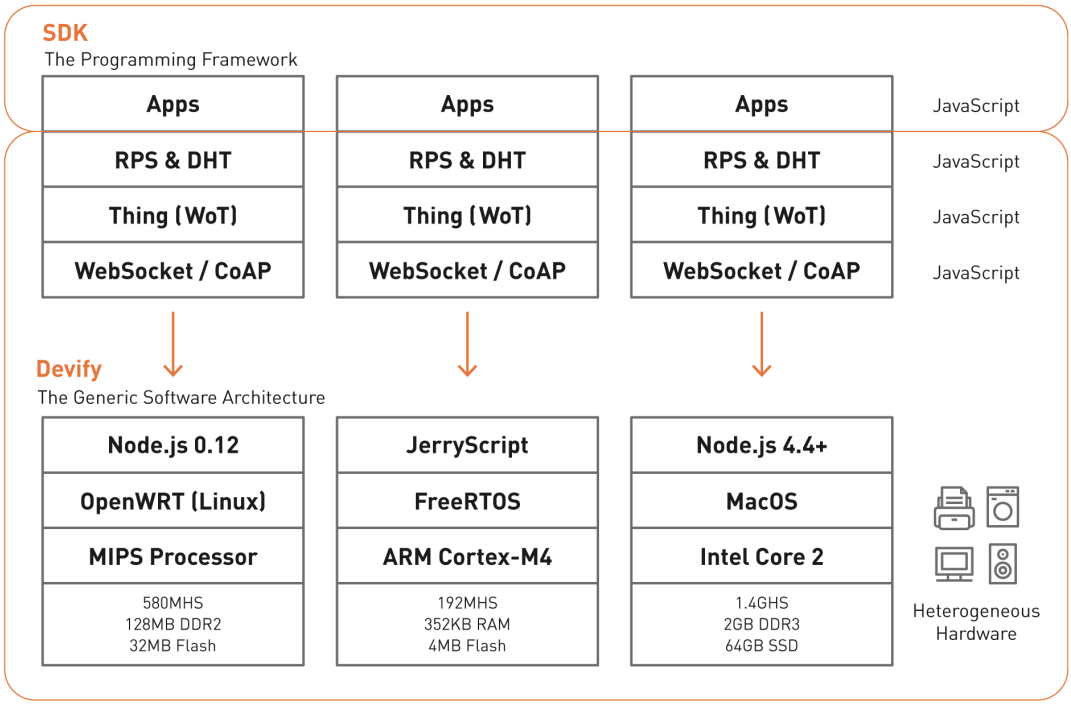
JavaScript is one of the most popular programming languages, and it is the leader in the "GitHub Popular Programming Languages" list, which is why Flowchain uses it as the primary language of Flowchain. Not only can JavaScript run on different hardware, but the entry barrier is low, allowing developers in IoT industries to customize their services and products easily, and then generate more computing tasks on the platform to attract Miners stationed to accelerate the growth of the Flowchain ecosystem.

Heterogeneous Hardware

The concept of heterogenous hardware is straightforward: a wide range of hardware devices. The goal of heterogeneous hardware is more straightforward - "Write once, run everywhere." For IoT Blockchain, it would be a vital issue to build a software framework that can be implemented and execute on a wide variety of hardware devices.

Using JavaScript to implement the IoT system is popular, but the more substantial reason is for Heterogenous Hardware. As shown in Figure 7, Flowchain and its underlying operating system (Devify) are 100% JavaScript implementations, which solves fundamental portability issues. With today's IoT Device hardware technology, Flowchain framework can run on Microcontroller, Microprocessor and Cloud Server.

Flowchain is a full-stack software framework, meaning that its implementation from the bottom to the top uses JavaScript.



【Figure 7】

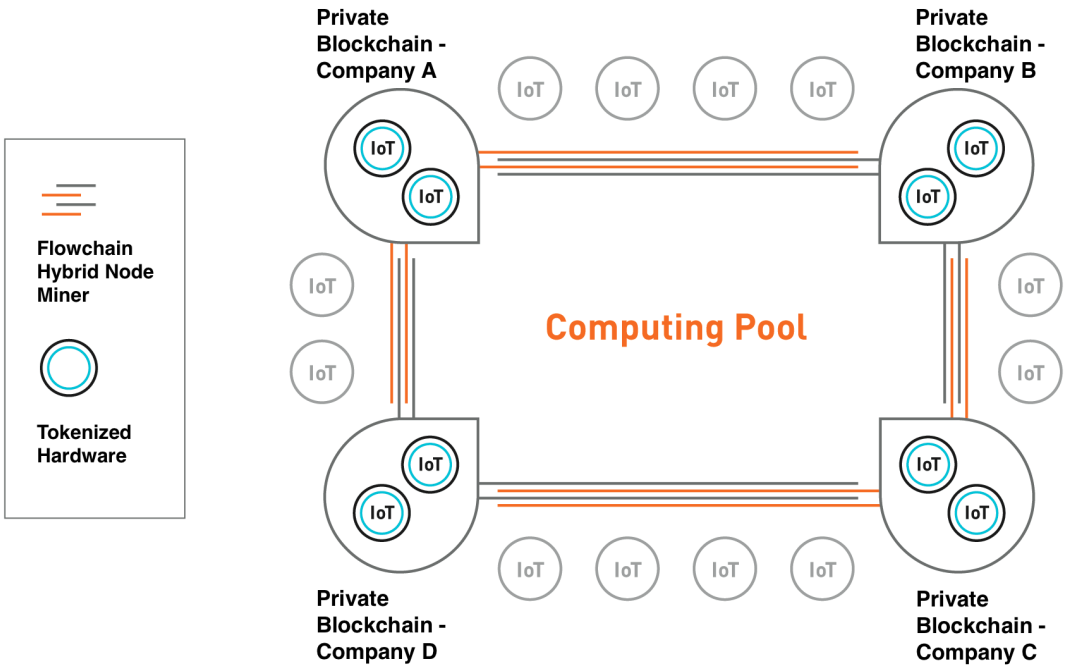
- **Web of Things Layer – How to connect between Edge Devices**

"Web of Things, WoT" is the application layer of IoT in Web technology. In short, it is the concept of adding "Uniform Resource Locator (URL)" to IoT - representing each device in URL over IoT network. In the decentralized IoT network, resources are managed by implementing the W3C's WoT standard. Just like the HTTP and Web protocols, the underlying IoT resources can be easily stored and read. Flowchain has been using the WoT concept since its inception and is the only IoT blockchain project to employ WoT concept in IoT firm.

- **Broker Server Layer – Conversion between public and private blockchains**

Flowchain is a hybrid blockchain architecture comprising of a public Proof-of-Work blockchain and multiple Proof-of-Stake private blockchains. The public blockchain allows the "miners" who are distributed around the world to participate freely without permission to providing AI computing power and mining "Pseudonymous Authentication" to receive block rewards. Also, surrounded by public blockchain, IoT

developers use the Flowchain SDK and the private blockchains of the IoT device equipped with Flowchain tokenized chips to provide collected information to the "miners" for calculation. The communication between miners and the IoT device employs the PPKI mechanism proposed by Flowchain and tokenized chips to validate the transactions of the information.



【Figure 8】

- **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.

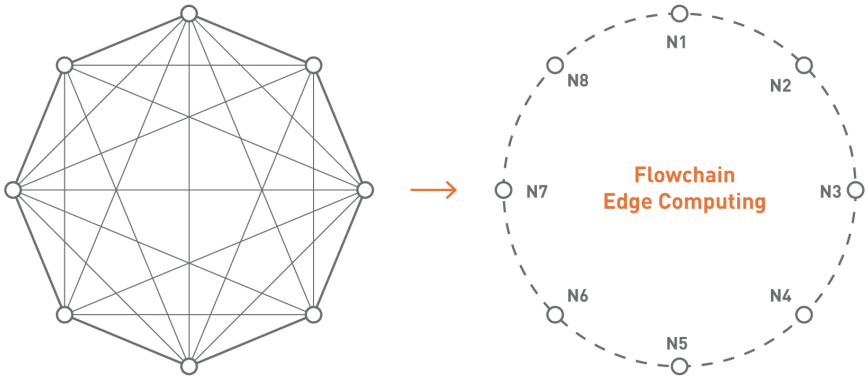
Flowchain's AI computing pool is built on the public blockchain. In addition to providing the Pseudonymous Authentication and computing capabilities required by Machine Learning and Data Analysis for IoT devices in the private chain, it also has essential attributes of the blockchain such as immutable, trusted data exchange, and permanent storage.

- **Private Blockchain**

Unlike public blockchains, only authenticated users can join the private blockchain network. The user needs to request permissions from an authority in the private blockchain for joining the network. The authority validates the authenticity of a user, and grant permissions to authenticated users for submitting transactions and accessing shared ledgers.

- **Peer-to-Peer IoT Networking**

Flowchain OS enables IoT devices to form a P2P (Peer-to-Peer) decentralized blockchain network. In addition to providing data model and data replicas capabilities for IoT and AI applications, it also ensures security for data and data trusted.



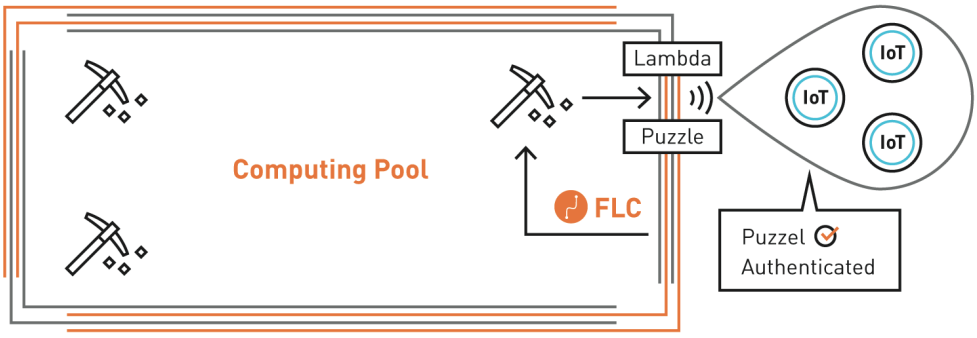
【Figure 9】

In such a ring structure, the MIT Chord algorithm is used as the node lookup and the location of the node to which the data belongs. The complexity is reduced from O(logN) to O(logN/2). Increase the speed of Lookup.

- **Hybrid Consensus Node**

As shown in figure 10, the Flowchain hybrid blockchain comprises of “private blockchain,” “hybrid consensus node” and “public blockchain” from the outside to the inside. The role of the "hybrid consensus node" is as follows:

1. Participation in the private blockchain's "Byzantine Fault Tolerance"
2. Responsible for "Identify" of IoT devices



【Figure 10】

Flowchain introduces "Pseudonymous Authentication" technology; the mechanism of "Pseudonymous Public Key Infrastructure (PPKI)[3]" is used to confirm the valid identity of the IoT device. The process is as follows:

1. Miners on the public chain produce a pair of "Puzzle" and "Lambda" values
2. Hybrid consensus node gets "Puzzle" and "Lambda" value from the public blockchain.
3. Hybrid consensus node broadcasts "Puzzle" to all IoT devices in the private blockchain
4. During the effective period of Puzzle, the IoT device that answers the puzzle answer at the same time can become "Authenticated" during this time.
5. Miners who assist in generating Puzzle and participating in the trusted device verification process will be rewarded with FlowchainCoin.

[3] Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks (J. Chen, 2018)。

- **Distributed Ledger Layer – API/SDK for developers**

"Decentralized applications (Dapps)" are computer programs consisting of smart contracts or programmatic self-execution protocols. Flowchain's Dapps are written in JavaScript and can be applied to different hardware to make IoT developers easily customizing their services and products.

Hardware | Flowchain Tokenized Chip - the key to organizing IoT Blockchain

The Flowchain tokenized chip, which was developed in collaboration with strategic partners, will be utilized by edge devices in the private blockchains. Subsequently, the Hybrid Node miners use PPKI, the PKI replacement proposed by Flowchain, to authenticate edge devices to enable them joining the Flowchain network. By joining the network, edge devices can submit data to the public blockchain. PPKI is Flowchain's unique security solution for IoT authentication. Section D describes the PPKI concept and algorithms.

D PPKI

Background

"Public Key Infrastructure"; also known as PKI is an information infrastructure consisted of hardware, software, participants, management policies and processes which designed to create, manage, distribute, use, store, and revoke digital credentials.

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.

In summary, there are hundreds of millions of devices on the IoT operating at the same time. If PKI is used as a consensus mechanism, it will consume huge resources and time, causing system paralysis. Therefore, Flowchain proposed PPKI in particular to replace the traditional PKI on the private blockchains.

Hybrid Blockchain and Use Cases

A hybrid blockchain comprises of public and private blockchains. The hybrid blockchain creates openness and trust of transactions in the public blockchain, and protect the privacy-sensitive data in the private blockchain. Such technique has already been proposed to secure blockchains and applied to digital rights management . The use cases of the hybrid blockchain are as follows.

1. In a hybrid blockchain, the private blockchain can determine which transactions are public, and submit these transactions to the public blockchain for open access.

2. In a hybrid blockchain, the public blockchain can store transactions to secure data provenance.

Based on the application design and business logic, the blockchain architect can use the public blockchain, private blockchain, or a hybrid model by leveraging the benefits of both public and private blockchains. To achieve a secure and inexpensive blockchain for the IoT, Flowchain introduces Hybrid Blockchain Architecture as shown in Figure 2 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 blockchain technology.

The miners on the public blockchain can ensure fast certification comes from the Edge Device on the private blockchain, speeding up the transfer of data to each other. PPKI is one of the innovative technologies of the Flowchain blockchain, and Flowchain is also the world's first blockchain to introduce PPKI technology.

Pseudonymous Authentication Method

As previously described, the distributed computing uses the full authentication technique such as the PKI to control access to their networks. Also, most existing blockchains use such PKI technique to authenticate users, secure the communications and verify transactions by multi-party computation[4]. However, the study[5] has figured that such PKI technique is too strong to enable a fast communication. Specifically, the IoT blockchain need to authenticate nodes with fast; as such, Flowchain proposes the

[4] S. Goldwasser and Y. Lindell. Secure multi-party computation without agreement. Journal of Cryptology, 18(3):247–287, 2005.

[5] J. Katz, A. Miller, and E. Shi. Pseudonymous broadcast and secure computation from cryptographic puzzles. 2015.

pseudonymous authentication technique to address such technical challenge. The pseudonymous authentication uses the technique of computational puzzles solving to replace the PKI to enable a fast authentication.

Moreover, such PKI technique is too strong that it involves confirming the identity of a user by validating the authenticity of a user with a digital certificate. Unlike a strong authentication technique, the user is anonymous in such pseudonymous authentication system, and the system validates the authenticity of the anonymous user by the consensus of the solution. The pseudonymous authentication uses a weaker but secures enough authenticity system. The blockchains such as Bitcoin which don't use strong authentication systems have proven the notion of pseudonymous authentication to be a tremendous success. In summary, figure 10 shows that IoT nodes in the hybrid blockchain network are pseudonymously authenticated in the private permissioned blockchain to ensure near real-time transactions.

Puzzle Miner Algorithm

The users, represented as IoT nodes in this paper, can join the private blockchain and submit transactions to the public blockchain by solving a computational puzzle mined by the miners. The puzzles are computed by miners in the public blockchain, and broadcasting to the private blockchains.

Flowchain hybrid blockchain uses a lottery function to generate Konami Code which can be used to verify the solution. Formally, let λ be Konami Code, a truly random magic string generated by the lottery function, and each puzzle is bound to this Konami Code. Let Fpuz be the puzzle solving function, and Ui represents each user.

Then, if the user does not submit the solution of the puzzle to the public blockchains within a fixed time interval, the public blockchain assumes that the user is unauthenticated. Also, the transactions submitted by the unauthenticated user are considered untrusted which can be discarded. Therefore, untrusted transactions will not

be recorded in the public blockchain. This paper assumes that the user can solve a puzzle within a fixed time interval σ, then the mining process of the miners is as follows.

Puzzle Miner Algorithm:

---

1. Ui starts receiving λ from the broadcasting
2. Let Puzzle be a function and §j be a string; Ui receives a puzzle (Puzzle, xj) from a peer Uj in the private blockchain over the p2p network
3. Let Puzzle(λ) gives an arbitrary-length vector ~x of the Konami Code, then ~x = (x1, . . . , xn), n < j
4. Let Fpuz maintain a set T of puzzle solutions, then Fpuz computes each entry in ~x, let yi = Fpuz(xi), i = (1, . . . , j)
5. The miners say that Ui solves the puzzle (Puzzle, xj) if Fpuz successfully finds yi = xj within the time interval σ
6. Fpuz returns §j to Uj and stores H = (~x, yi,) in T
7. The miners and Uj confirm the user Ui is authenticated

Also, the user U*i* can thus use H to sign transactions and submit the transactions to the public blockchains for verifying; the submit process be as follows.

Transactions Submit Process:

---

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 key pair (sk_i, pi_i); let S*ign* be the signature function
3. Let T*i* be the new transaction and H*ash* be a hash function so that T*i* = H*ash*(S*ign*(*M*), *H*, pk_i)
4. U*i* submits T*i* to the public blockchain

E Virtual Blocks

The blockchain for the IoT has considered an emerging technology for creating more secure and more cost-effective IoT systems. Despite a myriad of projects on blockchain IoT, few of them have investigated how an IoT blockchain system works in practice. In this paper, we introduce 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 chapter describes a detailed technical description of the proposed implementation.

The Purpose of Virtual Blocks

This section identify an apparent reason for Virtual Blocks to existing in Flowchain technologies. Bitcoin, a frequently referenced cryptocurrency, uses a distributed database system called a blockchain. The Bitcoin blockchain can operate without any central server that the transactions stored with high trust. As the Bitcoin blockchain uses “unverified pool” to queue new transactions, the average waiting time for verifying a transaction could be 15 minutes that not in a real-time manner. Thus, to address this technical challenge, the main aim of the Flowchain distributed ledger 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 mechanism called Virtual Blocks to provide such real-time transactions ability.

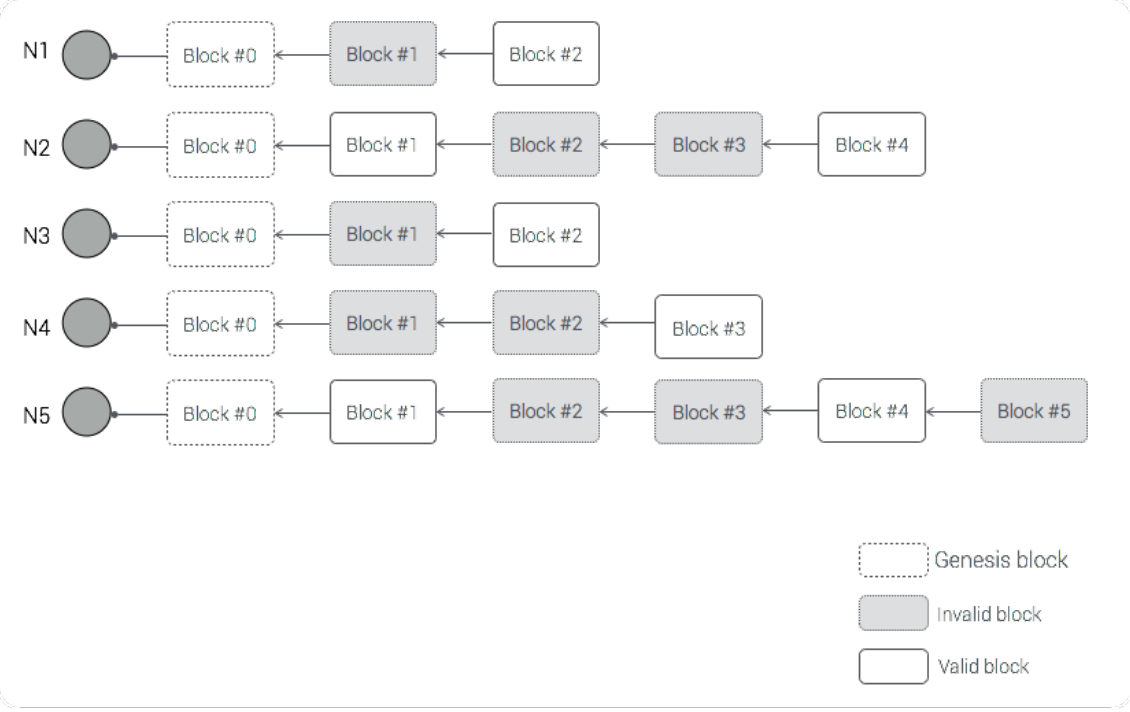
Moreover, IoT hardware varies, e.g., resource-constrained devices, mobile devices, and high-performance server frames that the computing power varies from devices.

Although memory-bound functions have been proposed to deal with such **heterogeneous hardware** to avoid “mining competition” and denial-of-service attacks, this technique cannot be employed in IoT devices. A resource-constrained device has limited computational power and memory resource; therefore, memory-bound hash functions do not perform well on such IoT devices. Consequently, the proposed Virtual Block system can also address such technical challenges.

Conceptual Framework of Virtual Blocks

Followed by figure 6, the proposed blockchain data structure is called Virtual Blocks, and it aims to provide real-time data transactions. Flowchain initially creates branches for each node when nodes mine their Virtual Blocks. This design can estimate the block “forks” exception during the mining process. In this way, Flowchain can act in a real-time manner through maintaining “valid and invalid blocks.”

【Algorithm 1】



As shown in Algorithm 1, the important Flowchain data structure design features are as follows.

1. Five IoT devices are labeled N1 to N5, and each device is a “node” in a peer-to-peer network.
2. All nodes are mining blocks that use the same genesis block.
3. In other words, each node creates a new “branch” for mining; thus, there is no blockchain “fork.”
4. Every block in each branch is called a Virtual Block.
5. Virtual Blocks can be labeled as valid or invalid.
6. Only valid blocks are available to record transactions.

The most significant design feature of the Flowchain data structure is that every node can only mine blocks at its branch. Therefore, Virtual Blocks do not need to be synchronized with all nodes because nodes do not “compete” to mine new blocks.

Process and Algorithm of Virtual Blocks

Technically, “mining” is a mechanism and distributed consensus system that can verify and record such transactions. In Flowchain, the Virtual Block system can label blocks as valid or invalid. Valid blocks act as a secure ledger that stores transaction records. Although Flowchain and Bitcoin use the same SHA-256 hash algorithm, Flowchain has a very different mining algorithm design. The proposed design allows an IoT device to operate more stably when mining blocks. As shown in Algorithm 2, a node receives a key-value pair through the peer-to-peer network and then stores it in a valid block.

【 Algorithm 2】

```
Node.on('message', function(key, value) {
  // Get a valid block of the device's blockchain
  N = GetOneValidBlock(chains)

  // Put key-value pair in block "N"
  PutToBlock( N, { key: value } );
});
```

【 Algorithm 3】

```
Difficulties = [
  '0000FFFFFFFFFFFF', // [0.0, 0.2)
  '000FFFFFFFFFFFFF', // [0.2, 0.4)
  '00FFFFFFFFFFFFFF', // [0.4, 0.6)
  '0FFFFFFFFFFFFFFF', // [0.6, 0.8)
  'FFFFFFFFFFFFFFFF'  // [0.8, 1.0)
]
```

Moreover, Flowchain will use the probability distribution as a mechanism to update the mining difficulty and thus Flowchain can have a cost-effective mining system.

1. Reliability probability - A probability calculation can directly reference an IoT device's "reliability."

2. Probability density - Use the reliability as the variance input of the probability density function.

Furthermore, to facilitate a faster and more cost-effective mining algorithm, a predefined difficulty table can easily implement such an algorithm. For example, the leading zeros will increase the degree of difficulty. The mining becomes increasingly difficult with more leading zeros. Algorithm 3 shows that the miner can simply search the difficulty table and pick a value according to the probability.

The miner labels new virtual blocks found as valid, and as any invalid condition occurs, the current in use virtual block becomes invalid. Invalid virtual blocks are treated as deleted, and they will no longer become valid again.

The invalid conditions can vary between different types of IoT hardware. For example, the operating system on a resource-constrained device may enter the starvation status due to the resource leaks. In general, invalid conditions are dependent on a result from such starvation problems, application process abnormal termination (e.g., crash, restart), the operating system exceptions (e.g., out of memory, out of disk space), and the program errors, such as the network disconnection error.

Also, to reduce the complexity of maintaining valid and invalid blocks, Listing 3 shows an O(1) implementation that labels the latest block as a Most Recently Used (MRU) block; thus, every IoT device will have only a single valid block.

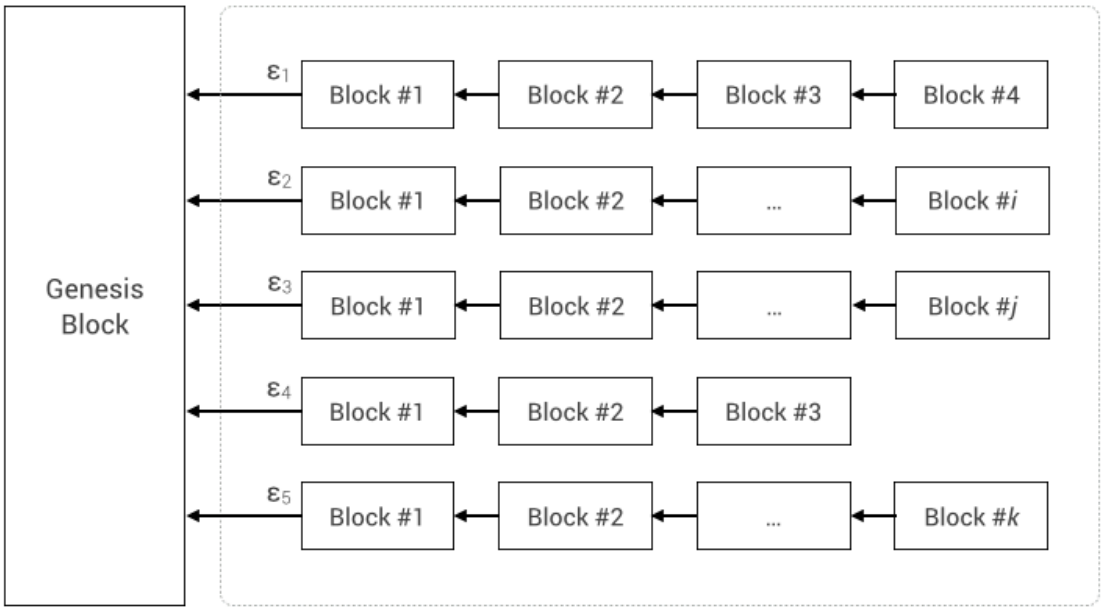
【Algorithm 4】

```
Node.on('message', function(key, value) {
  // N is the length of the blockchain.
  // Put payload in the latest block in the blockchain.
  // This is to say; only the latest block is valid for use.
  PutToBlock( chains[N-1], { key: value } );
});
```

In theory, these systems can simply condition the impossibility of starvation, abnormal, exceptions and errors as mentioned earlier so that Flowchain can employ this single valid block model.

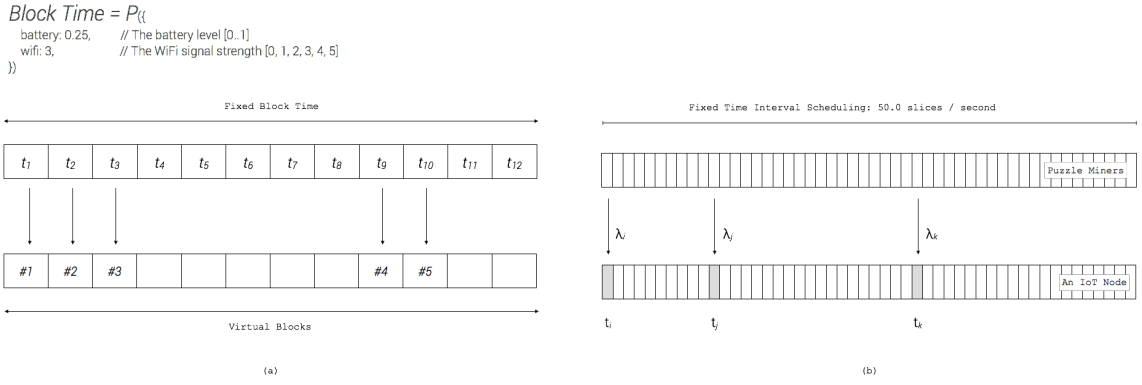
Virtual Blocks Miner

【Algorithm 5】



This section describes the algorithm of the virtual block miner. As previously described, Flowhain can build a private blockchain that the IoT devices can self-organize as a p2p network. Every Flowchain IoT Node in the private blockchain has a local blockchain that keeps the privacy-sensitive data. Algorithm 5 depicts the concept of virtual blocks and the local blockchain. The local blockchain starts from the genesis block and is chained by virtual blocks mined by a local miner executing on the IoT node.

【Algorithm 6】



【Algorithm 7】

1. The block time is determined by *P*, the Poisson distribution function
2. The value of *P* is resulted by *stakes* such as the battery level and WiFi signal strength
3. At the time *t1*, *P* predicts that if the termination time of the current block is exactly *early* than the end of *t1*, than *block #1* is successfully mined
4. The local miner continues to step 2 and 3 to mine more virtual blocks

Flowchain comprised a mining-based proof-of-stake model for IoT devices that the block time, the time to find a valid block, is predictable and can be timed in a fixed number calculation per second. Furthermore, Kraft and Daniel[6] studied the predictable block times for various hash-rate scenarios as the Poisson process with time-dependent intensity. Therefore, we model the prediction of block times as a Poisson probability density function to ensure a cost-effective difficulty control system. Algorithm 6(a) depicts the concept of this mining process.

In Algorithm 6(a), the local miner predicts that *block #2* can be found at *t2*, and *block #4* can be found at *t9*. The block time of *block #4* is *longer* than expected because that the WiFi signal is weak at time *t4* to *t8*.

Virtual Blocks Consensus Algorithm

This section describes the consensus algorithm of virtual blocks miner.The Byzantine agreement is a consensus algorithm to avoid distort data[7] across p2p nodes. Technically, the Byzantine agreement is a distributed decision-making process that some amount of nodes are agreed on transactions and can replicate the data; such a

[6] D. Kraft. Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications, 9(2):397–413, 2015.

[7] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4(3):382–401, 1982.

mechanism is also known as *fault-tolerance.*, and Byzantine agreement is known as Byzantine Fault-Tolerant (BFT). Therefore, the private blockchain can also agree on the *private transactions* by fault-tolerance, meaning that the p2p network in the private blockchain can replicate a certain of private transactions.

In general, if a maximum number of *n* node can distort data, a BFT algorithm can be achieved with a total of *3n+1* nodes to tolerate the network. However, if nodes can not distort application data submitted through them, then an amount of *2n+1* nodes is capable of tolerance the network. There are various BFT implementations such as Practical Byzantine Fault-Tolerant (PBFT)[8], and Speculative Byzantine Fault Tolerant (Zyzzyva)[9] can be employed in the private blockchains of our hybrid model. The implementation is a selection according to the difference in their business logic.

As described previously, we present a *local miner* by which virtual blocks are mined. Moreover, the genesis block is pre-defined by the private blockchain developers. As Algorithm 5 previously figured that the genesis block, formally denoted as *G*, which is pre-defined by private blockchain developers, and there are give entities *ε1*, *ε2*, *ε3*, *ε4*, and *ε5* in a private blockchain. As such, Algorithm 6(a) depicts the process of local mining, and the following example shows *ε1*.

1. The public blockchain has σ slices per second, meaning that the puzzle miner uses a fixed time interval mining mechanism
2. The puzzle miners in the public blockchain are broadcasting *λ1* at time *t1*
3. The Flowchain node *ε1* has a sensory data, formally denoted *M*, and *ε1* generates a transaction *T1* =*Hash*(*Sign*(*M*), *H*, pk*i*)

[8] M. Castro and B. Liskov. Practical byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation, OSDI '99, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association.

[9] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong. Zyzzyva: Speculative byzantine fault tolerance. SIGOPS Oper. Syst. Rev., 41(6):45–58, Oct. 2007.

4. The Flowchain node *ε1* successfully mines *Block #1* after *Fpuz* solving the puzzle bound with *λ1*, and stores *t1* in virtual block *Block #1* of *ε1*
5. *ε1* repeats steps 2, 3, and 4, until the end of σ slices and resulting in a total number of 5 transactions, [*T1*,..., *T5*], which were stored in virtual block *Block #1*
6. *ε1* subsequently continues to get *λ2* at *t1*, as well as resulting in 10 transactions, [*T6*,..., *T15*], which were stored in virtual block *Block #2*
7. At the time *t3*, the IoT node *ε1* submits [*T1*,..., *T15*] in the virtual blocks, *Block #1* and *Block # 2*, to the private blockchain network
8. All authenticated nodes in the private blockchain can join the consensus activity to agree on [*T1*,..., *T15*], that all the transactions will become *trusted*
9. The BFT consensus can ensure that trusted transactions [*T1*,..., *T15*] were replicated in the private blockchain, meaning that the private blockchain is capable of *fault-tolerance of private trusted transactions.*

Algorithm 6(b) shows such local mining technique that the Flowchain node was pseudonymously authenticated to submit transactions at (t*i*, t*j*, t*k*). Furthermore, the above process also gives the *deferred submission* concept. The Flowchain node can *gather* transactions in its virtual blocks and submit *gathered* transactions to the public blockchain in a future time.

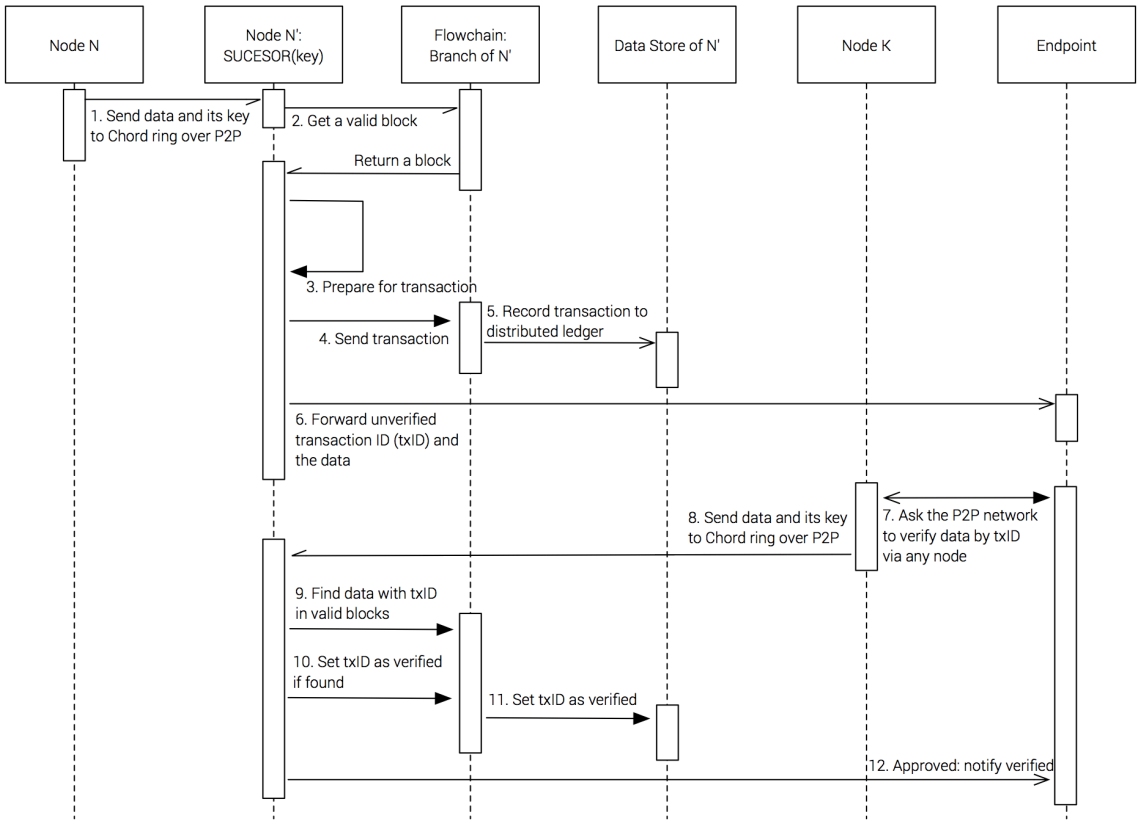
Virtual Blocks Approval Sequence

Flowchain uses a “mining-transaction-approval-verify” process which forwards the transactional data to the endpoint before verification rather than the typical “transaction-mining-verify” process.

Regarding the process (6) of Algorithm 8, N’ forwards the chunk data to the endpoint after recording the transaction in the distributed ledger. At this time, Flowchain will not

label this transaction as a “verified transaction.” Subsequently, in the process (7), the endpoint requests “approval” via one node of the peer-to-peer network. The previously mentioned transaction will only become a verified transaction if the peer-to-peer network successfully verifies it. In conclusion, Flowchain will recognize the transaction as a verified transaction when the endpoint requests to approve it. Thus, the Flowchain transaction process represents a “mining-transaction-approval-verify” model. This mechanism is the most important Flowchain design element.

【Algorithm 8】



Algorithm 8 shows the process (11) that N’ marks txID as verified after completing the approval request of the endpoint. Then, Flowchain grants one FlowchainCoin token to N’. Note that N’ can obtain more FlowchainCoin by completing more approval jobs. In this manner, Flowchain comprises a resource-based proof-of-stake mining approach to mine new blocks. An IoT node can deposit “tokens” by joining and completing “approval” jobs. The miner ensures the node’s minimum resource requirements, such as network bandwidth, battery level, Wi-Fi signal strength, and the “coins.” Thus, the Flowchain

difficulty algorithm uses the number of tokens held by a node along with the resource requirements to calculate the reliability probability. In short, **IoT nodes need to hold a few amount of FlowchinCoin tokens in order to join the consensus process and submit their data transactions.**

Peer-to-Peer Trusted Computing

Flowchain's virtual blocks subsystem is responsible for real-time transactions and recording trusted data. Also, the Flowchain distributed ledger treats each data slice (the "chunk" data) in a time series or streaming data as a separate transaction, and Flowchain IoT nodes transfer each transaction to the peer-to-peer network for consensus. As such, Flowchain employs the Chord algorithm to exchange chunk data over the peer-to-peer network.

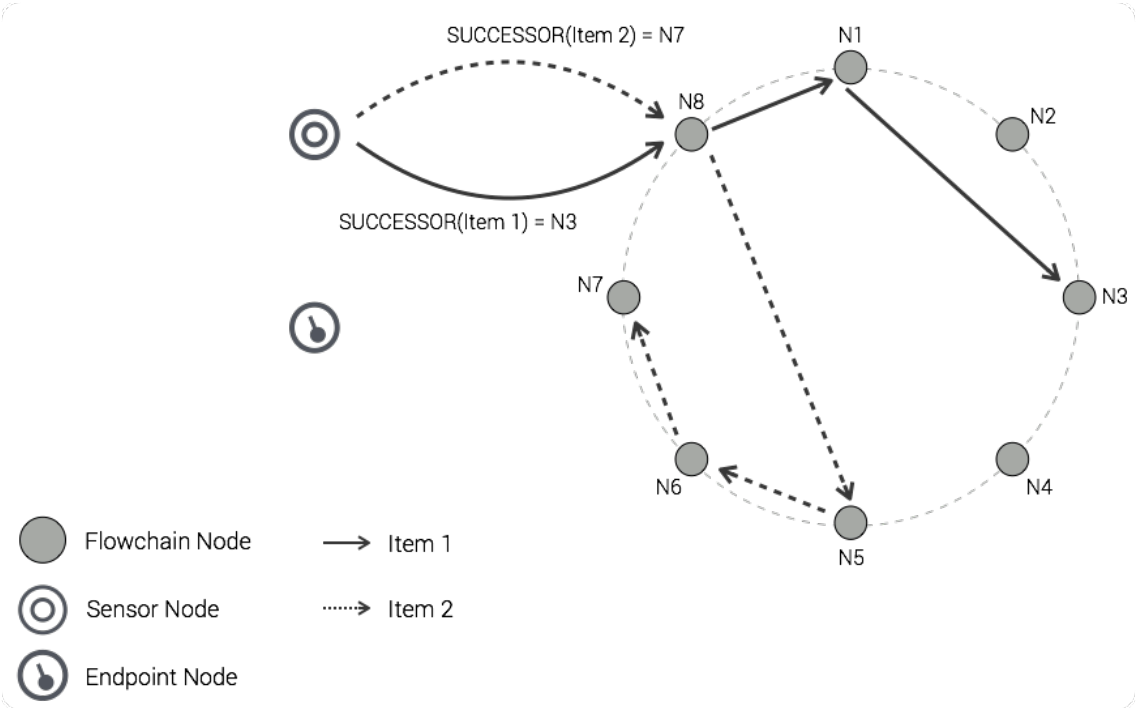
Each data slice is hashed by a double SHA-256 hash function to the corresponding data "key." Chunk data comprise sliced data and the data key. Then, Flowchain IoT nodes forward the chunk data to the chunk data's "successor" node over the Chord ring. The Chord protocol and algorithm organize all IoT devices as a peer-to-peer network in a "ring" topology. The successor node lookup via the DHT with the data key processes the chunk data: Create a new transaction from the chunk data and store it in a valid block after verification.

Algorithm 9 shows the successor(key) function of the Chord algorithm that finds the data key's node through the peer-to-peer network. The successor node is represented as N'. When N' receives the chunk data, it combines the valid block ID and the data key to generate a transaction ID. To ensure data privacy, N' can also sign the transaction with its private key embedded in the hardware. Finally, N' creates a record that comprises the transaction ID and the chunk data and stores the record in a valid block.

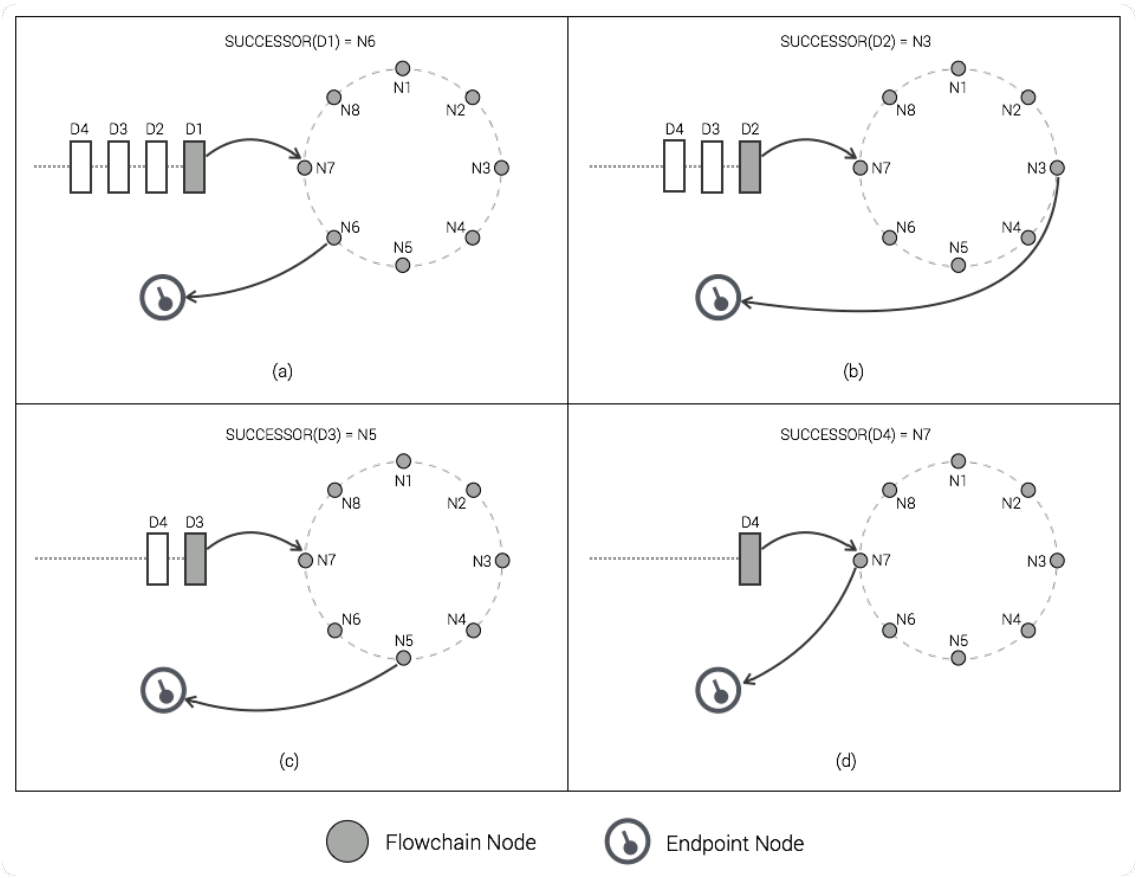
Security Considerations

Obviously, given the data key's hash generation algorithm, it is natural that the successor node is random and difficult to predict. In other words, the time series and streaming data are stored and distributed across IoT devices. Algorithm 10 simulates four transactions from a time-series that each transaction is forwarded to the peer-to-peer network in sequence. Regarding the simulation process, it is evident that the successor node of each transaction is unpredictable. Thus, this design helps to ensure data security. In summary, Flowchain can ensure the IoT data security by using this chunk data model in which the distributed ledger stores transactional data across different IoT devices.

【Algorithm 9】



【Algorithm 10】



Object Storage for Time-Series Data

Flowchain distributed ledger technology proposes a Linked Data document to support time series database (TSDB) via the semantic web technology. Time series data stored across the distributed ledgers requires the ability of fast access to the data store and retrieve, thus, Flowchain uses JSON-LD as the primary linked data technology to structure the transaction into a simple key-value document to make access to data more efficient. Furthermore, several studies[10] [11] have presented NoSQL databases as the high-performance key-value stores; thus, Flowchain uses Google LevelDB[12], a

[10] Forfang, C., Bratsberg, S.: Evaluation of High Performance Key-Value Stores (2014).

[11] Cattell, R.: Scalable SQL and NoSQL data stores. ACM SIGMOD Record. 39, 12 (2011).

[12] LevelDB, http://leveldb.org

lightweight NoSQL database, as the backend engine to implement such TSDB technology.

【Algorithm 11】

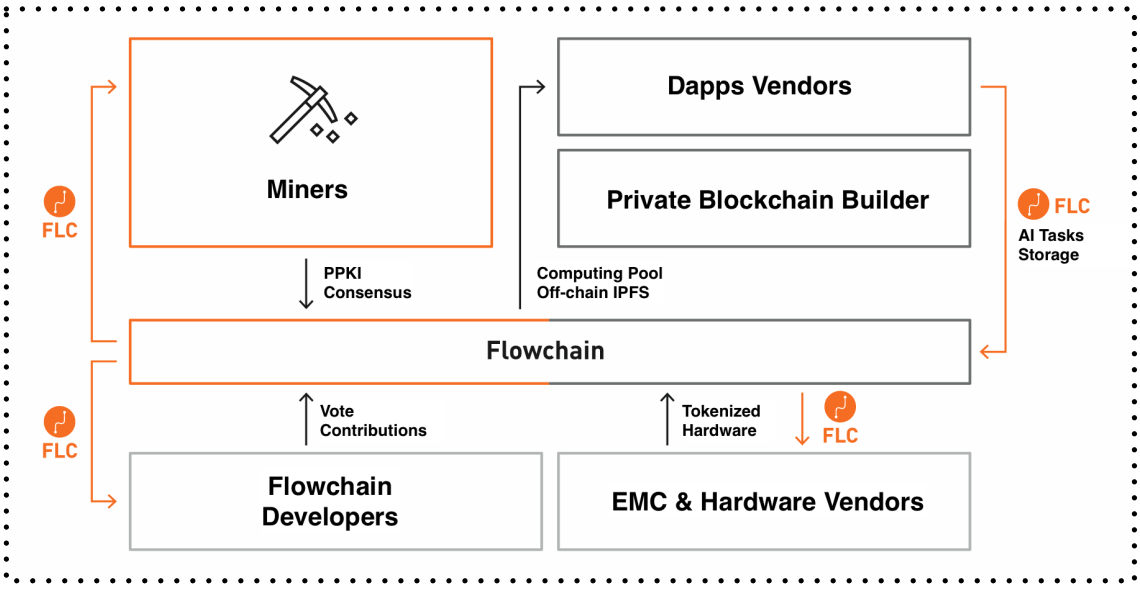
```
N'.PutToBlock(block, doc) {
  db = DatabaseAdapter.getDatabase();

  txID = SHA256( SHA256( block.id + doc.key ) );

  tx = new Transaction( doc.value );
  tx.sign( privateKey );

  record = {
    "@context": "http://flowchain.io/ledger-context.jsonld",
    "txID": txID,
    "tx": tx
  };

  db.put( record );
}
```

Algorithm 11 shows that the IoT node N' presents a transaction record in the JSON-LD document format. The use of Linked Data for Distributed Ledgers together with a NoSQL engine as the TSDB backend ensures the data access efficiency.

F Flowchain Ecosystem

Ecosystem Overview - "Partners" and "Platform Users"

In the ecosystem of Flowchain platform, different roles need to be involved to create a new blueprint for AI + IoT. Participants are mainly divided into "cooperating partners" and "platform users"; the former includes "EMC manufacturers" and "Flowchain developers", while the latter includes "Dapp developers", "private blockchain builder" and "miners".



【Figure 11】

Alliance for Software and Hardware Integration - EMC Vendors

In the Flowchain ecosystem, EMC vendors as partners will work with Flowchain –

1. Develop Flowchain tokenized chips for Edge Device of IoT Blockchain

2. Providing the initial computing power of the platform - EMC manufacturers will build private computing centers, which will be put into the Flowchain network during the idle period of operation to provide computing power.

Contributors to improve the platform - Open source developers

Flowchain is a "platform model" based on Blockchain technology. Compared to "product" or "service", it requires more manpower to develop and maintain. Therefore, Flowchain will invest an amount of money to set up a software foundation to build its own developer community, inviting all the best players to improve and complete the Flowchain function.

Collaborators to support the network - Miners

In Flowchain ecosystem, miners get block rewards (referred to as FLC) by completing the AI computation and consensus tasks assigned by the computing pool. The task details are as follows:

1. Participate in the AI computing tasks assigned by the computing pool and contribute the ide GPU computing power
2. Participate in the Flowchain public blockchain network to ensure that the public blockchain has sufficient GPU computing power and generate secure "Puzzle" and "Lambda" with PPoW technology, making the PPKI mechanism stronger.
3. When the miner is not assigned to the AI computing task, the Ethereum can still be used for mining, effectively utilizing the idle computing power.

In the distribution model of Flowchain Token, 70% of the max token supply will be issued in Token Distribution Layer (virtual mining). The concept is as follows:

1. Expect to use public mining model for establishing the community of sharing computing power for the AI and IoT
2. The public mining model can establish a more reliable way of issuing tokens. And also reduce possible fraud and investment in speculation.

In addition, Flowchain's virtual mining mechanism also uses "Stake" as the basis for AI computing task assignments.[13]

1. The miner can convert the Ethereum token (ETH) mined during the idle time of Flowchain public blockchain mining to FLC.
2. The conversion process will be through the Ethereum smart contract, which will leave a transaction record on the Ethereum public blockchain. The conversions are considered as the stake of the Flowchain miner.
3. Miners with higher stakes will have the priority of AI computing tasks assignments.

Innovators to strengthen the ecosystem - Dapp vendors

In the past, developers who stayed outside the industry because of "computing power" and "electricity" can now enter the IoT industry with relatively low development and operating costs to develop their IoT products and services because of the strategic layout of Flowchain on software and hardware.

[13] Jollen Chen. 2018. Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks. SIGBED Rev. 15, 5 (November 2018), 22-28. DOI: https://doi.org/10.1145/3292384.3292388

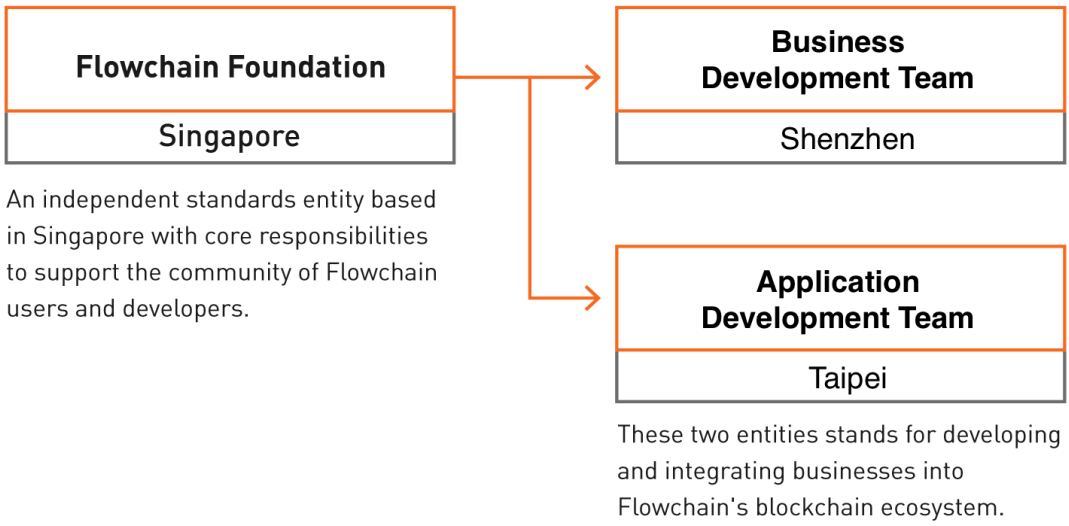
G Flowchain Team

Flowchain is an IoT blockchain open source project from Taiwan and is operated by the Flowchain Foundation. The Flowchain core team is based in Taiwan and includes open source contributors, part-time consultants and academic partners from the world.

Flowchain Core Team	
Jollen Chen	Founder and CEO
Angelina Huang	PR and Marketing Lead
Junus Chen	General Counsel
Patrick Lo	Operations Lead
Jin Wang	Business Lead of Greater China
Ellaine Lin	Project Manager
Ben Shiue	Open Source Team
Archer Huang	Open Source Team
Red One	Open Source Team
Polo Wu	Open Source Team
Roy Chen	Open Source Team

H Flowchain Foundation

The Flowchain Foundation has three offices in Singapore, Taipei and Shenzhen, which are responsible for different businesses, as shown in the figure -



【Figure 12】

Flowchain Foundation is based in Singapore and is responsible for Flowchain community support and global marketing efforts, with Flowchain founder Jollen Chen as CEO. The office in Shenzhen with the management team Jin and Chalmers is responsible for business development in China. The office in Taipei is responsible for delivering Flowchain IoT solutions to global.

The Flowchain Foundation is also responsible for the planning and supervision of the use of Flowchain digital assets and managing Flowchain working capital; the use of Flowchain working capital will be discussed by the Flowchain Foundation's budget committee and will be based on integrity, openness, fairness and transparency. ◦

Digital Assets

The tokenized hardware technology provided by Flowchain enables the intelligent data on the IoT Network to be converted into valuable digital assets via the Flowchain network, the digital assets are called FlowchainCoin (FLC).

As a digital asset of Flowchain, FLC will ensure the security and correctness of data by means of tokenized IoT hardware. It can also make precious digital assets to be transferred quickly and securely under without any third party.

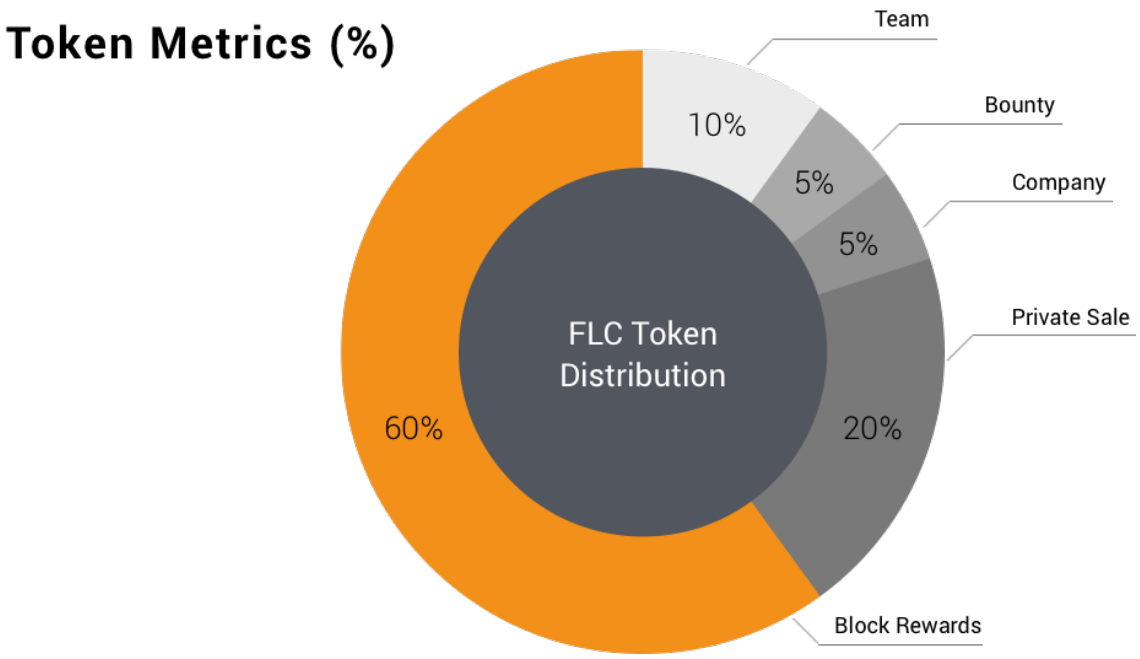
Name	FlowchainCoin
Symbol	FLC
Type	Utility Token / Dapps Token
Contract Address	0x5b53f9755f82439cba66007ec7073c59e0da4a7d
Supply	1,000,000,000
Platform	Ethereum / ERC-20

FLC Token Type

FlowchainCoin (FLC) token is a Utility Token, sold in Ether as a forward purchase of Flowchain products and services. It can be transferred to other individuals or entities freely. The token holders purchase FLC Tokens at a discounted price during the private sale period and can resell the FLC tokens to other players for them to purchase the products and services at a market price.

Token Distribution - Token Metrics

Flowchain encourages the community to support the network by participating in the activities of the Flowchain network. Thus, we use the Ethereum Distribution Layer technology to distribute most of the FLC tokens. The Distribution Layer adopts the public mining mechanism to reward mining nodes. Please refer to the following table for FLC token metrics. Figure 13 shows the FLC token distribution metrics.



【Figure 13】

Team	10%	Incentives for the founder and genesis team
Bounty	5%	Building and reward for the community
Company	5%	Reserve for marketing, advisors reward, and business development
Private Sale	20%	Long-term project funding
Block Rewards	60%	Incentives for nodes to join Flowchain mainet

Private Sale Planning

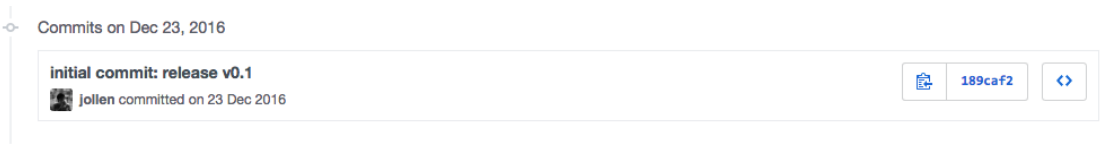
The Flowchain project didn't have ICOs and this section describes the schedule plan of private sales.

Private Sale, 5% of the total supply, is allocated to fund project development. We consider the funds for each stage of development.

Stage	Details	Schedule
Presale	• Price: 1 ETH = 6400 FLC • KYC needed • Limited to accredited investors • Token distribution: immediately	Start: June 1, 2018 Close: July 1, 2018
Private Sale A	• Price: 200 TUSD = 5000 FLC • KYC needed • Accredited investors • 1-Year Lock / 1 Month Cliff / Monthly vest	Start: December 1, 2018 Close: January 1, 2019

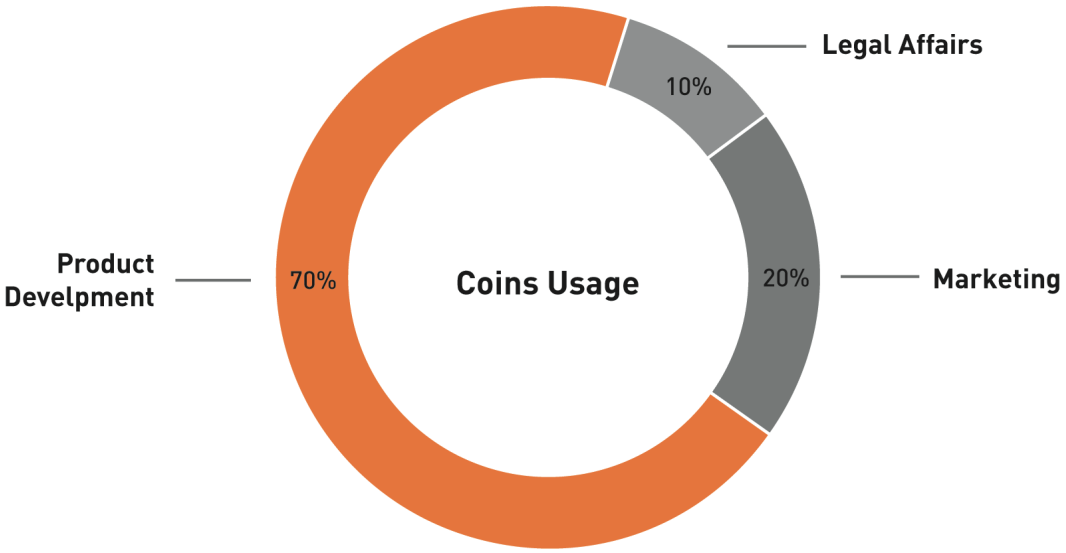
Private Sale B	• Planned to launch on April 1, 2019 • Price: TBD • KYC / AML needed • Accredited Investors and Partners • 2-Year Lock / 6 Month Cliff / Monthly vest
Private Sale C	• Planned to launch on October 1, 2019 • Price: TBD • KYC / AML needed • Accredited Investors and Partners • 3-Year Lock / 6 Month Cliff / Monthly vest
Private Sale D	• Planned to launch on December 1, 2019 • Price: TBD • KYC / AML needed • Accredited Investors and Partners • 3-Year Lock / 6 Month Cliff / Monthly vest

The Flowchain project started in 2015, from 2015 to 2017, the project has published several peers reviewed papers to support its technology and methodology. The initial working prototype was committed on December 23, 2016, by Jollen, the creator of Flowchain. Please refer to https://github.com/flowchain/flowchain-ledger/tree/189caf2625b82d3459dcd7ee611bfcc36afde2be for the initial commit (hash: 189caf2625b82d3459dcd7ee611bfcc36afde2be).



Also, a working testnet has already launched on June 26, 2018, along with a comprehensive open source project accessible at https://github.com/flowchain. The

Private Sale A was closed on December 31, 2018, that the token holders can access the open source project and the testnet. The live network is operational before the private sale. Figure 14 shows the budget allocation of funds.



【Figure 14】

Token Distribution Layer - Public Mining

FlowchainCoin (FLC) is the digital assets of valuing Flowchain networks. As previously described, the FLC can tokenized hardware to enable digital assets exchange without any central party, meaning that FLC token is a kind of hardware crypto token to protect your data and ensure data privacy. Technically, Flowchain uses FLC as the crypto technology to ensure data trust that would be the originators of the data.

The token metrics show that FLC can be distributed as block rewards by public mining. Figure 15 shows there are three types of nodes that can mine FLC by participating in the Flowchain network.

- **Hybrid Node Miner (Edge Node Miner)**

In the Flowchain network, edge node miners have to join the Flowchain mining pool and contribute their network bandwidth to broadcast puzzles to IoT devices.

- **IPFS Node Miner**

In the Flowchain network, IPFS miners have to join the Flowchain mining pool as well and contribute their storage to deploy Flowchain dapps and store dapp data.

Flowchain Dapp, which integrates Flowchain and IPFS DAG distributed technology, is responsible for validating transactions of streaming data and store the streaming data in IPFS network.

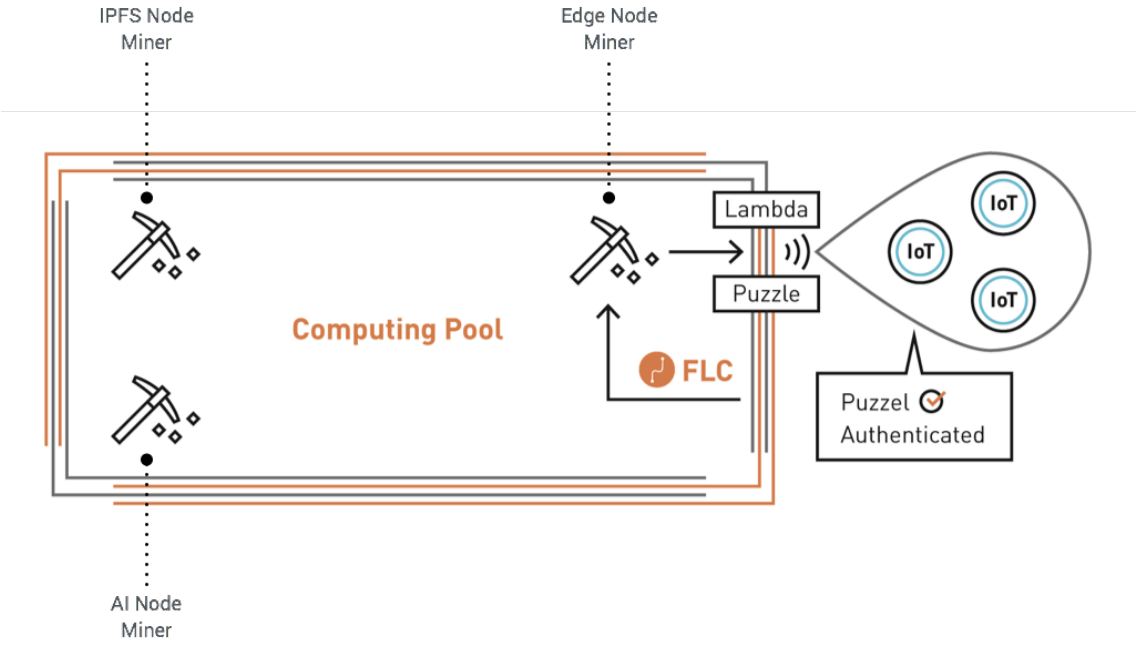
The integration of Flowchain/IPFS has been tested on the Flowchain Testnet. The Flowchain network can combine with IPFS nodes to process live video streams.

How Flowchain/IPFS Works	
Flowchain	Provides Virtual Blocks technology to handle chunked data
IPFS	Distributed storage and retrieval
Flowchain+IPFS	Flowchain hybrid blockchain technology interactives with IPFS Merkle DAG
Flowchain/IPFS Dapps	The application layer of Flowchain+IPFS
IPFS Node	Execute Flowchain dapps

- **AI Node Miner**

In the Flowchain network, AI node miners have to join the Flowchain mining pool as well and contribute their GPU compute power to execute Flowchain dapps.

From the perspective of block rewards, users can lease their excess computing power and free storage space (the “Resources”) through the Flowchain network and get FLC as block rewards. Hybrid node miners, IPFS node miners, and AI node miners that contribute resources on Flowchain Network can receive such block rewards.



【Figure 15】

Token Usage

FLC is the only way to access Flowchain Network. FLC holders have to deposit FLC in Flowchain hardware to proof the “stake” in order to access Flowchain Network. By accessing Flowchain Network, the hardware can run Flowchain Miner to participate in public mining for block rewards. We’ve already shipped two such products listed below.

Flowchain/IPFS Network Storage Solution	AI Mining Inc offers an enterprise-class network storage solution based onFlowchain and IPFS. The solution can store real-time data streams on IPFS nodes through Flowchain distributed ledgers. It is especially suitable for video live broadcast and media streaming applications. Please visit https://aimining.io for more product information
Mooncake	To embrace the future of 5G and IoT Edge Computing, AI Mining and Maker Diary provide “Mooncake” development kits for IoT developers. Mooncake has a built-in Flowchain OS that supports Bluetooth, Thread, IEEE 802.15.4, 2.4GHz and other wireless communication protocols. For developers interested in IoT blockchain technology, Mooncake can be used as an Edge Computing node and become a Flowchain hybrid node in Flowchain hybrid blockchain network. Please visit https://aimining.io for more product information

Purchase and Use FLC

FlowchainCoin (FLC) tokens are traded on the following major digital assets exchanges. Please visit https://flowchain.co/flc/tokenize.html for information on how to use FLC.

Exchange	Market	Direct Link
Digifinex	FLC/ETH	https://www.digifinex.com/en-ww/trade/ETH/FLC
IDAX	FLC/USDT	https://www.idax.pro/#/exchange?pairname=FLC_USDT
BitMart	FLC/BTC	https://www.bitmart.com/trade/en?symbol=FLC_BTC
	FLC/ETH	https://www.bitmart.com/trade/en?symbol=FLC_ETH

Please visit https://flowchain.co for future exchange updates.

- **Wallet**

We suggest MetaMask or Trust Wallet manage your FLC tokens. These popular wallets can protect your digital assets with high security.

- **Risk Notice**

Risk Notice A private key is necessary to control and dispose of FLC stored in your digital wallet or vault. Accordingly, loss of requisite private key(s) associated with your digital wallet or vault storing FLC will result in loss of such FLC. Accordingly, the value of FLC tokens is currently very volatile. Flowchain Foundation does not have any means of recovering lost tokens or stabilizing the token value, buy at your own risk.

- **Legal Disclaimer and Token Sale T7C**

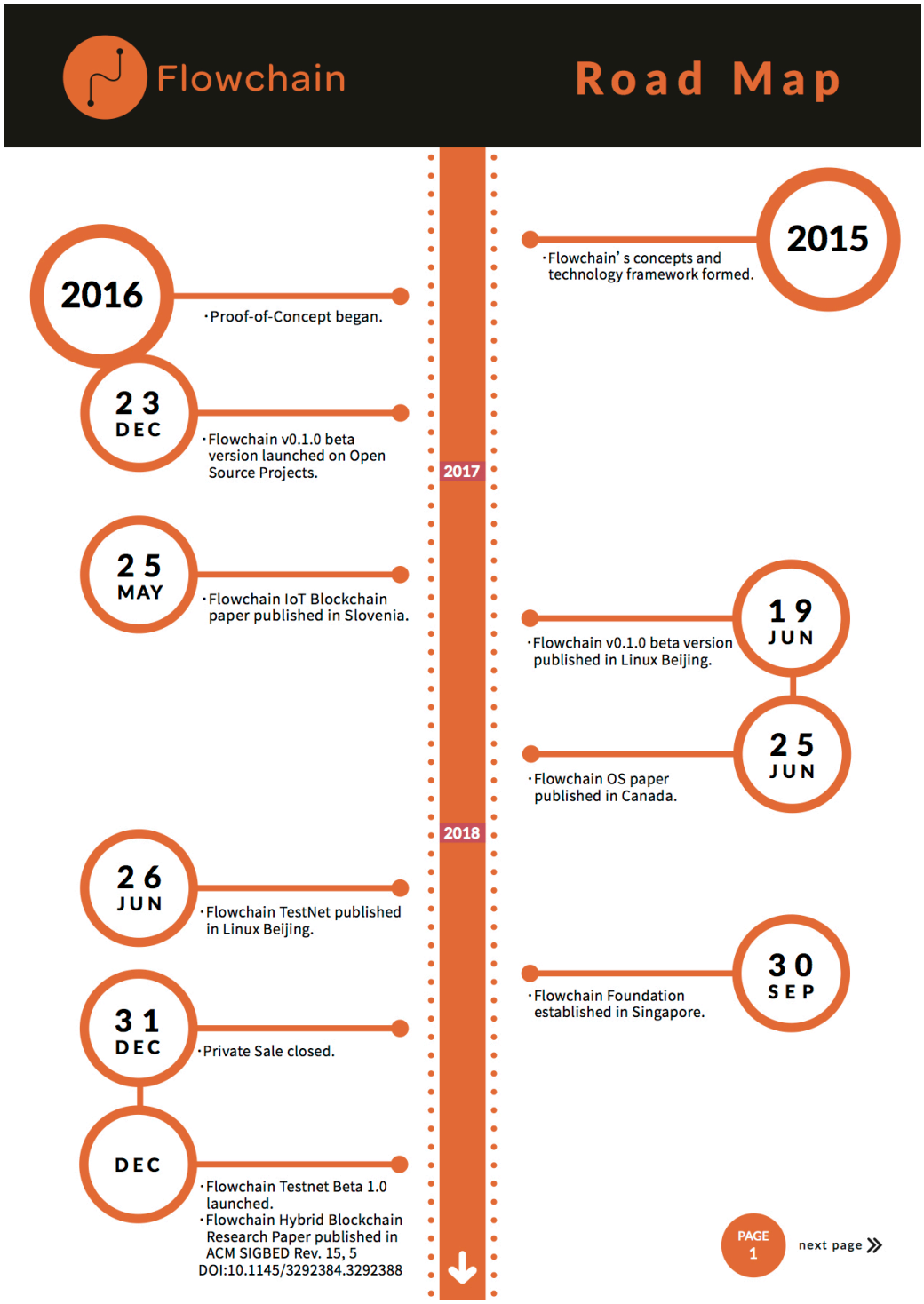
Please visit https://flowchain.co/documents/index.html for Legal Disclaimer and FLC Token Sale Terms and Conditions (T&C) and Risk Notice.

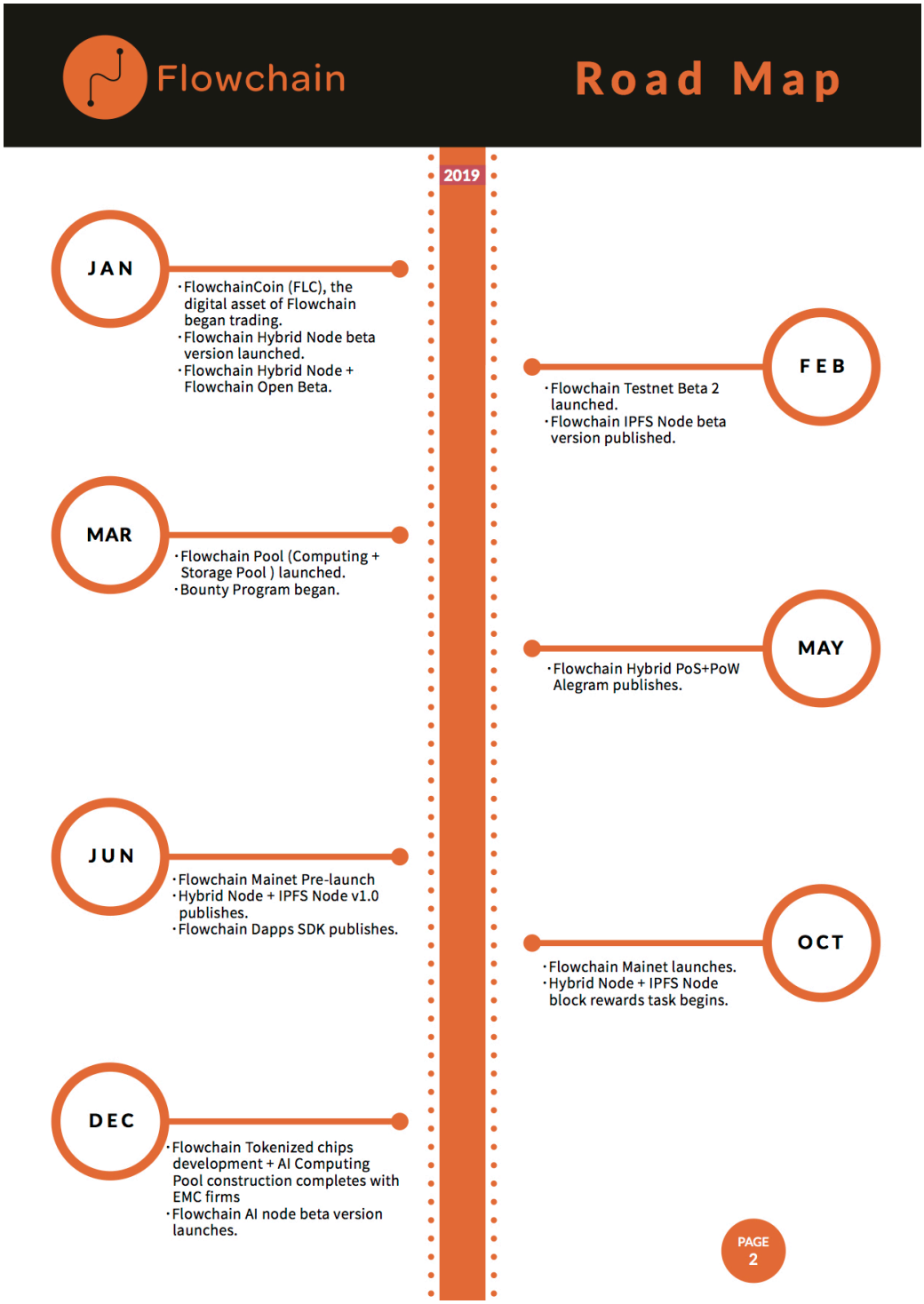
Howey Test

This paper has already made detailed Howey Test according to A Securities Law Framework for Blockchain Token. Our overall risk score is 0, which is very unlikely to be considered as a security.

Please refer to Appendix A for Howay Test Report.

J Roadmap





K Conclusion

According to IDC reports in 2018, real-time data represents 15% of the datasphere in 2017 and almost 30% by 2025. The increasing need for real-time data will profoundly affect the user experiences and should be addressed with a better IoT improvement. Overall, the Flowchain IoT Blockchain solution provides a dedicated blockchain system for the IoT that can ensure data security on a promise of real-time transactions. The report also indicates that nearly 90% of all data created in the global datasphere by 2025 will require some level of security, but less than 50% will be secured. This significant gap would threaten the data reality that opens up new vulnerabilities to private/ sensitive information and the value of data mining. In short, the specific challenges in the IoT blockchain market are that enterprises can't guarantee their data security and privacy. Thus, Flowchain utilizes the emerging blockchain technology in the IoT solutions to resolve the problems and bring solutions to our clients. In summary, our enterprise clients can benefit data security and privacy by adopting Flowchain IoT solutions. Our offering can bring two unique benefits as listed below.

1. Provide data security and privacy by adopting Flowchain private blockchain technologies.

2. Provide the data assets capability of enterprise data. The Flowchain "tokenized hardware" technology can tokenize enterprise sensitive information and the valued data as digital assets and store the assets on the public blockchain.

We are ready to ship IoT devices with Flowchain OS, also expect to deliver enterprise edge solutions with Flowchain hybrid blockchain in Q2, 2019.

Please visit https://flowchain.co for whitepaper updates.

Appendix A Flowchain Howey Test

Element 1: Investment of Money

Is there an investment of money?				
Characteristic	**Points**	**Explanation**	**Examples**	**Y or N**
There is no crowdsale. New tokens are given away for free, or are earned through mining	**0**	Tokens which are not sold for value do not involve an investment of money. For example, if all tokens are distributed for free, or are only produced through mining, then there is no sale for value.	There was never any token sale for Bitcoin. The only way to acquire new bitcoin is via mining. A token which is randomly distributed for free	**Y**
Tokens are sold for value (crowdsale)	**100**	Tokens which are sold in a crowdsale, at any time, regardless of whether sold for fiat or digital currency (or anything else of value) involve an investment of money	A token which is sold for bitcoin in a crowdsale. A token which is sold for ether in a crowdsale.	**N**

Total for Element 1 **0**

Element 2: Common Enterprise

What is the timing of the sale?				
Characteristic	**Points**	**Explanation**	**Examples**	**Y or N**
Pre-deployment	**70**	A sale of tokens before any code has been deployed on a blockchain is more likely to result in a common enterprise where the profits arise from the efforts of others. This is because the buyers are completely dependent on the actions of the developers, and the buyers cannot actually participate in the network until a later time.	A developer has an idea for a new protocol, writes a white paper and does a crowdsale.	**N**
The protocol is operational on a test network	**60**	If there is a functioning network there is less likely there is to be a common enterprise where the profits arisef rom the efforts of others. The closer the sale is to launch of the network, the less likley there is to be a common enterprise.	A developer has an idea for a new protocol, writes a white paper and deploys a working test network before doing a crowdsale.	**N**
Live network is operational	**50**	If the token is sold once there is an operational network using the token, or sold immediately before the network goes live, it is again less likely to result in a common enterprise	The crowdsale is done at the same time the network is launched.	**N**

What do token holders have to do in order to get economic benefits from the network?				
Characteristic	**Points**	**Explanation**	**Examples**	**Y or N**
All token holders will always receive the same returns	**25**	If returns are paid to all token holders equally (or in proportion to their token holdings) regardless of any action on the part of the token holder, then their interests are more likely aligned in a common enterprise	'HodlToken' holders are automatically paid an amount of ETH each week, based on fees generated by other users of the network 'FoldToken' does not pay any return, and there is no way to earn more tokens within the network (but they can be bought, sold or traded)	**N**
There is a possibility of varying returns between token holders, based on their participation or use of the network	**-20**	If token holders' returns depend on their own efforts, and can vary depending on the amount of effort they each put in, then there is less likely to be a common enterprise	'CloudToken' holders can earn more tokens by providing data storage on the network, or can spend tokens to access data storage. Holders who do not provide data storage do not earn any more tokens.	**Y**

Total for Element 2 **-20**

Element 3: Expectation of Profit

What function does the token have?				
Characteristic	**Points**	**Explanation**	**Examples**	**Y or N**

Ownership or equity interest in a legal entity, including a general partnership	**100**	Tokens which give, or purport to give, traditional equity, debt or other investor rights are almost certainly securities. ***If one or more of these characteristics apply, the token is almost certainly a security, notwithstanding the results of the other elements***	A developer releases and sells 100 'BakerShares' tokens. Each token entitles the holder to 1 share in Baker, Inc. A developer releases and sells 100 'BakerProfit' tokens. Each token entitles the holder to 1% of the profits of Baker, Inc. for the next year. A developer releases and sells 100 'BakerDebt' tokens. Each token entitles the holder to principal and interest repayments based on the initial token sale price.	**N**
Entitlement to a share of profits and/or losses, or assets and/or liabilities	**100**			**N**
Gives holder status as a creditor or lender	**100**			**N**
A claim in bankruptcy as equity interest holder or creditor	**100**			**N**
A right to repayment of purchase price and/or payment of interest	**100**			**N**
No function other than mere existence	**100**	A token which does not have any real function, or is used in a network with no real function, is very likely to be bought with an expectation of profit from the efforts of others, because no real use or participation by token holders is possible. Voting rights alone do not constitute real functionality.	A developer releases and sells 100,000 'SocialCoin' tokens to fund the development of a new Social Network. However, SocialCoin is not required to access the network and has no real function after the sale.	**N**
Specific functionality that is only available to token holders	**0**	A token which has a specific function that is only available to token holders is more likely to be purchased in order to access that function and less likely to be purchased with an expectation of profit.	'CloudToken' is the only way to access and use a decentralized file storage network.	**Y**

Does the holder rely on manual, off-blockchain action to realize the benefit of the token?				
Characteristic	**Points**	**Explanation**	**Examples**	**Y or N**
Manual action is required outside of the network (e.g. off-blockchain) in order for the holder to get the benefit of the token	**80**	A token whose value depends on someone taking specific manual action outside of the network means that the token is not functional in and of itself. Instead, the token relies on a level of trust in a third party taking action off-blockchain. This sort of token is more likely to be bought for speculation - i.e. the expectation of profits.	A developer releases and sells 'FreightCoin', which will allow the holder to pay FreightCoin to access capacity on a new real-world freight network. The network relies on legal contractual relationships and manual actions. (This alone does not make FreightCoin a security)	**N**
All functionality is inherent in the token and occurs programmatically	**0**	A token which is built with all the necessary technical permissions means that the token holder does not rely on manual actions of any third party. This means that the buyers are more likely to purchase the token for use rather than with the expectation of profit from the efforts of others.	Holders of 'SongVoteToken' can sign transactions on the network as votes for their favorite new songs and earn rewards for doing so.	**Y**

What is the timing of the sale?				
Characteristic	**Points**	**Explanation**	**Examples**	**Y or N**
Pre-deployment	**20**	A sale of tokens before any code has been deployed on a blockchain is more likely to result in buyers purchasing for speculative reasons with the expectation of profit, rather than practical use cases.	A developer has an idea for a new protocol, writes a white paper and does a crowdsale.	**N**
The protocol is operational on a test network	**10**	If the sale occurs after code has been deployed and tested, the token is closer to being able to be used	A developer has an idea for a new protocol, writes a white paper and develops a working test network before doing a crowdsale.	**N**
Live network is operational	**0**	If the token is sold once there is an operational network using the token, or immediately before the network goes live, it is more likely to be purchased with the intention of use rather than profit.	The live network is launched before the crowdsale.	**N**

Can the token holders exercise real and significant control via voting?				
Characteristic	**Points**	**Explanation**	**Examples**	**Y or N**
Token holders as a whole are able to control the development team's access to funds	**-20**	If the collective approval of token holders is required in order for the development team to access the funds raised in the crowdsale, then any value realized by the token holders is more closely tied to their own decisions, and less reliant on the efforts of others.	A development team sells 100,000 Tokens for a total of 100,000 ETH. 50,000 ETH will be released from the token contract to the development team immediately, but the remainder is only released once milestones are met, which requires approval of a majority of the token holders each time. If the milestones are never met, the remaining ETH will be returned to the token holders.	**N**

Token holders as a whole are able to vote on significant decisions for the protocol	**-10**	If the collective approval of token holders is required in order to make significant changes to the protocol, then any value realized by the token holders is more closely tied to their own decisions, and less reliant on the efforts of others.	Changes to the protocol require a vote by token holders.	**N**

Note: Voting rights must be in addition to functionality. A token with voting rights alone and no other real functionality is very likely to satisfy element 3

How is the token sale marketed?				
Characteristic	**Points**	**Explanation**	**Examples**	**Y or N**
Marketed as an 'Initial Coin Offering' or similar	**50**	It is not possible to prevent some buyers from buying a token purely for speculation. However, marketing the token as an investment leads buyers to believe they can profit from holding or trading the token, rather than from using the token in the network. Using terms like 'Initial Coin Offering' or 'ICO', and investment-related language like 'returns' and 'profits' encourages buyers to buy a token for speculation, rather than use.	'ProfitCoin' includes potential of 'high ROI' and 'investor profits' in its marketing material.	**N**
Marketed as a Token Sale	**0**	Marketed as a sale of tokens which give the right to access and use the network		**Y**
There is no economic return possible from using the network	**-100**	If there is genuinely no economic return possible for the token holders, then there is unlikely to be a common enterprise. This will be rare.	Backers contribute to a cause and receive a 'thank you' token which has no economic value.	**N**

Results

Guide		**Your results**	
Total Points	**How likely is the element to be satisfied?**		
0 or less	Very unlikely	Total for Element 1	**0**
1 - 33	Unlikely	Total for Element 2	**-20**
34 - 66	Equally likely and unlikely	Total for Element 3	**0**
67 - 99	Likely		
100 or more	Very likely	**Overall Risk Score**	**0**

A token will only be a security if it satisfies all three elements. The higher the point score for each element, the more likely the element is to be satisfied.

For many blockchain tokens, the first two elements of the Howey test are likely to be met. The third element has the most variables and the most different outcomes depending on the characteristics of the particular token.

Important notes

Please remember that this methodology produces nothing more than an estimate. The Overall Risk Score and the categories of likelihood are a guide only.

The Howey test has not yet been directly applied by the courts to any digital currency or blockchain token. The Howey test as applied by the courts does not involve any points-based calculation. The points system is intended as a guide - to highlight the characteristics of a token which are relevant to the securities law analysis.

This Framework should be read together with the full legal analysis. This Framework and the full legal analysis may be updated in the future as the law in this area develops.

You should not rely on this Framework as legal advice. It is designed for general informational purposes only, as a guide to certain of the conceptual considerations associated with the narrow issues it addresses. You should seek advice from your own counsel, who is familiar with the particular facts and circumstances of what you intend and can give you tailored advice. This Framework is provided "as is" with no representations, warranties or obligations to update, although we reserve the right to modify or change this Framework from time to time. No attorney-client relationship or privilege is created, nor is this intended to be attorney advertising in any jurisdiction.

Last updated December 7, 2016